universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Fermat Pseudoprime Numbers

verfasst von

Birgit Trappl, Bakk.rer.nat. BSc

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag.rer.nat.)

Wien, 2013

Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Mathematik
Betreut von:	ao. Univ.-Prof. Dr. Christoph Baxa

Abstract

The purpose of the Diploma thesis at hand is to provide a proper compendium on different types of Fermat pseudoprimes. The choice of this topic is motivated by its great significance in cryptography or more precisely in primality testing. Furthermore, standard literature in number theory and cryptography seldom deals extensively with numbers of that kind and they are usually examined in texts concerning computational number theory or cryptography, in which the main focus is on algorithms and efficiency of primality testing. Within the scope of this work Poulet numbers, Fermat pseudoprimes, Carmichael numbers, Euler pseudoprimes, strong pseudoprimes as well as superpseudoprimes are discussed in a more abstract and theoretic way in terms of definition, properties and distribution.

Zusammenfassung

Das Ziel der vorliegenden Diplomarbeit ist eine Übersicht über verschiedene Typen von Fermat Pseudoprimzahlen zu geben. Die Wahl dieses Themas gründet sich in seiner großen Bedeutung im Bereich der Kryptographie beziehungsweise der Primzahltestung. Weiters finden sich in der Standardliteratur über Zahlentheorie und Kryptographie nur selten ausführliche Informationen zu diesen speziellen Zahlen, denn sie werden meist in Werken über computergestützte Zahlentheorie und Kryptographie erläutert, wobei hierbei das Augenmerk hauptsächlich auf die Algorithmen und Effizienz der Primzahltests gelegt wird. Im Rahmen dieser Arbeit werden Poulet-Zahlen, Fermatsche Pseudoprimzahlen, Carmichael-Zahlen, Eulersche Pseudoprimzahlen, starke Pseudoprimzahlen sowie Superpseudoprimzahlen im abstrakteren und theoretischeren Kontext in Hinblick auf Definition, Eigenschaften und Verteilung besprochen.

Acknowledgements

First of all I would like to express my gratitude for the overwhelming patience of my advisor ao. Univ.-Prof. Dr. Christoph Baxa and of course for his professional advice and support. Furthermore, I feel a need of thanking ao. Univ.-Prof. tit. Univ-Prof. i.R. Dr. Johannes Schoißengeier and Univ.-Prof. i.R. Dr. Heinz Mitsch, who both inspired me in various lectures on algebra and number theory to get involved in these topics.
In addition I will always owe my gratitude to my family for their financial and emotional support. Moreover I would like to thank Bernd Gallner, Denise Schuster and Karoline Mühlbacher for their encouragement and emotional backing.

Contents

Introduction

Nowadays public-key cryptography gained great significance in everyday life, especially in the field of internet security. One of the most common public-key system is the RSA-algorithm, which is based on the factoring problem, meaning the problem to factorize an integer into its prime factors. Whereas multiplying huge prime numbers can be done pretty fast, factoring large integers is very difficult. Therefore it is necessary to determine bigger and bigger primes to ensure that prime factorization of large integers cannot be done in appropriate time. The largest prime number presently known is $2^{57885161} - 1$ (17 425 170 digits), which was discovered on 25 January 2013 by Great Internet Mersenne Prime Search (GIMPS) volunteer Curtis Cooper's computer in Orlando, Florida according to [WWWa, WWWb] .

In order to seek for primes with ever increasing digits several tests were devised, but as mentioned before factorization methods like trial division are inefficient and therefore quite expensive for large numbers as noted by [Chi09, p.206] and [Rie94, p.85]. Overcoming this naive approach and its drawbacks different kinds of tests were prospected and many of them are based on **Fermat's little Theorem** because of their efficiency. In [Rie94, p.84] a basic differentiation between compositeness and primality test was suggested. According to the author a successful primality test proves an integer N to be prime and if it fails, it proves an integer being composite. In contrast to that compositeness tests of course prove an integer N being composite if they are fulfilled, but if the condition of this test is not fulfilled, then primality of N is not necessarily proven. This and the fact that those methods do not give any indication on factors of N are quite big disadvantages in comparison to factoring methods, which can accomplish both although taking much more time. Because of predominating drawbacks of factorization methods those other classes of compositeness/primality tests are, nevertheless, used notwithstanding some composite integers passing the test. Besides causing wrong results in primality testing those special composite integers share some interesting properties with "real" prime numbers. Therefore they constitute an interesting and for already mentioned reasons an also important field of study in number theory resp. cryptography. This class of exceptional composites are generally called "**pseudoprimes**" for obvious reasons.

It should be noted, that there are several different types of pseudoprimes according to different primality tests. This Diploma thesis covers the field of Fermat pseudoprimes including some special types, which are discussed one subclass a section. However, there should be pointed out, that there are more general classes of pseudoprimes, like Lucas pseudoprimes (including Fibonacci pseudoprimes, strong Lucas pseudoprimes, extra-strong Lucas pseudoprimes, etc.) and even more general Frobenius pseudoprimes.

The reader should also be aware of problems in various notations and different definitions in literature for pseudoprimes in common and for Fermat pseudoprimes in particular. In this thesis those different notations would be pointed out in each section when defining the several pseudoprime types.
Despite the significance of pseudoprimes in computational issues of number theory and cryptography this Diploma thesis will be mainly focused on abstract and formal aspects of the concept of pseudoprimes. The structure of this work is due to proceeding to even more special types of Fermat pseudoprimes associated with even more specialized primality tests. In each section, after defining the distinct types, properties and distributions resp. infinitude of that type will be discussed.
However, for historical reasons the first section is about **Poulet numbers**, which are special types of Fermat pseudoprime numbers themselves, namely to the base 2.
In section 2 the notion of Poulet numbers is generalized to **Fermat pseudoprimes** for arbitrary bases $a \in \mathbb{N}$.
The following section 3 deals with **Carmichael numbers**; a very crucial type of Fermat pseudoprimes, since they would pass Fermat's primality test for any base a.
In order to resolve this disadvantage of Fermat's primality test more specialized tests will be suggested in the three sections 4 to 6. They also lead to other types of pseudoprimes, which are named after the corresponding tests **Euler Pseudoprimes**, **strong pseudoprimes**, and **superpseudoprimes**.
For more fluent reading preliminaries in number theory, analytic number theory and cryptography are sourced out into the corresponding appendices at the end.
For the purpose of this work the scheme below is a modification of a graphic found in [Guy04, p.44, Fig.3] . It shows the relationships of different types of pseudoprimes discussed in this thesis. Those connections will be explicitly and formally determined in the appropriate sections.

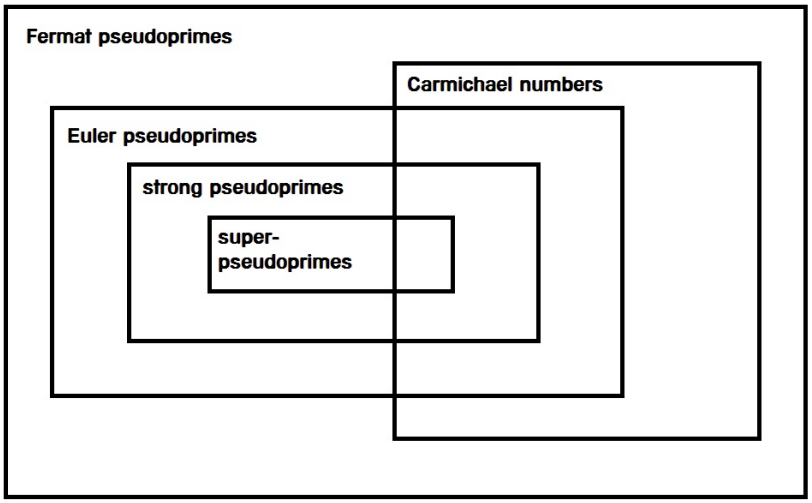

Figure 1: pseudoprime relationship scheme

1 Poulet Numbers

As indicated in the introduction at the beginning there should be considered some historical background concerning the concept of pseudoprimes especially in view of Poulet numbers, which are according to [KLS01, p.131] the earliest and most widely studied pseudoprimes. A quite detailed report on historical confusions concerning this topic can be found in [Rib04, p.88*ff*]. It is also mentioned by [KLS01, p.131] that it has been reported in several sources (see, for example [Dic52, p.59] or [Jea98]) that the ancient Chinese as long ago as 500 B.C. believed that

$$2^n \equiv 2 \pmod{n} \tag{1.1}$$

holds if and only if n is a prime number. This statement is (of course just in the sufficient direction) a special case of Fermat's little Theorem (see A.5).

According to [Rib04, p.88] this mistake has been perpetuated by several Western scholars. In Dickson's History of the Theory of Numbers, [Dic52, Vol. I, p. 91,] it is quoted that Leibniz believed to have proved that the so-called Chinese congruence indicated above implies that n is prime. Further there is a cross reference in [KLS01, p.131] to [Mah13], where it can be read that in September 1680 and also December 1981, Leibniz stated erroneously that congruence (1.1) holds only if n is prime.

Nevertheless (1.1) is true for integers $n \leq 300$, but as it is noted by [Rib04, p.90], [Sie88, p.229], and [KLS01, p.131] the first counter example $n = 341 = 11 \cdot 31$ was found by Sarrus in 1819 (see [Dic52, p.92]). In [Sie88, p.229] a short proof is carried out:

In fact, since 11 and 31 are odd primes, by Fermat's little Theorem (A.5) we have $2^{10} \equiv 1 \pmod{11}$ and, clearly, $2^{10} \equiv 1 \pmod{31}$. Hence $2^{341} \equiv 2 \cdot 2^{340} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$. Therefore number $2^{341} - 2$ is divisible by 11 and by 31, and so it is divisible by the product $11 \cdot 31 = 341$" , which means $2^{341} \equiv 2 \pmod{341}$.

[KLS01, p.131] listed the first eight composites fulfilling (1.1), which are 341, 561, 645, 1105, 1387, 1729, 1905, and 2047. In 1926 Poulet computed such composites in a table up to 5×10^7, and in 1938 [Pou38] up to 10^8 as it is cited by [Rib04, p.90].

1.1 Definition

Due to the fact that the Chinese congruence is a special case of Fermat's little Theorem the 2-pseudoprime test is a subclass for the more general notion of a-pseudoprime test, which is based on Fermat's little Theorem and will be discussed in section 2. Following [Chi09, p.206] we state the contrapositive of Fermat's little Theorem:

If a is some number coprime to n so that $a^{n-1}-1$ is not divisible by n, then n is not prime.

For purpose of this section let $a = 2$ and the **2-pseudoprime test** is a compositeness test of the following form:

If $2^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.

***Example* 1.1.** *[Chi09, p.206]* We can show, for example, that 9 is not prime, by observing that $2^8 \not\equiv 1 \pmod 9$ and using Fermat's theorem: if 9 were prime, then 2^8 would be congruent to 1 (mod 9): since it is not, 9 cannot be prime.
But we cannot conclude that 561 is prime by determining that $2^{560} \equiv 1 \pmod{561}$ (which is true), because in fact 561 is not prime - it is clearly divisible by 3.

[Chi09, p.206] further notes that as a test for compositeness of a number n, seeing if $2^{n-1} \equiv 1 \pmod{n}$ can be done rather quickly and is surprisingly effective, especially "as a first step in testing primality" [Rib04, p.90]. However, even if a randomly chosen number that satisfies the 2-pseudoprime test is likely to be prime, that conclusion does not necessarily apply to special types of numbers - the associated pseudoprimes, which will be defined in the following.

Definition 1.2.

(Version a) as in *[Rib04, p.90], [Chi09, p.207]*
A composite number $n \in \mathbb{N}$ satisfying the congruence $2^{n-1} \equiv 1 \pmod{n}$ is called *pseudoprime number (to base 2)*.

(Version b) as in *[KLS01, p.131], [Sie88, p.229]*
A composite number $n \in \mathbb{N}$ satisfying $n|2^n-2$ is called *pseudoprime number (to base 2)*.

***Remark* 1.3.**

(i) Nomenclature:
(see [Rib04, p.90], [KLS01, p.131], [Sie88, p.229], and [Chi09, p.207])
Since Sarrus figured out the first number of this type they are sometimes called *Sarrus numbers*. Similarly as those numbers was the focus of Poulet's attention they are often referred to as *Poulet numbers* (see [Dup53]). Another barely common term is *almost prime* (see [Erd50]). Consulting the following Section 2 on Fermat pseudoprimes it will be obvious naming them *pseudoprime number (to base 2)*, *2-pseudoprimes* or for short simply *pseudoprimes*.

(ii) Versions: There occur two versions of definition in literature. The difference will be discussed in Remark 2.2 for the even more general case of Fermat pseudoprimes.

1.2 Properties

In this subsection some properties of Poulet numbers shall be discussed. After general statements on Poulet numbers three special classes are mentioned, namely even pseudoprimes, Mersenne numbers and Fermat numbers. The last two special sets seem to be quite natural candidates for being pseudoprime numbers, since especially Mersenne numbers are used for achieving new prime number records.

As it is mentioned by [Rib04, p.91] in 1936 Lehmer [Leh36] gave criteria for the product of two or three distinct odd primes to be a pseudoprime:

- The product p_1p_2 is a pseudoprime if and only if the order of 2 modulo p_2 divides $p_1 - 1$ and the order of 2 modulo p_1 divides $p_2 - 1$.
- If $p_1p_2p_3$ is a pseudoprime, then the least common multiple of ord$(2 \mod p_1)$ and ord$(2 \mod p_2)$ divides $p_3(p_1 + p_2 - 1) - 1$.

Theorem 1.4. *[KLS01, p.133] If N is an odd pseudoprime, then $2^N - 1$ is also an odd pseudoprime.*

Proof. Since N is composite, there exists an integer c, $1 < c < N$, such that $c \,|\, N$. Then

$$2^c - 1 \,|\, 2^N - 1,$$

and $2^N - 1$ is also composite. It now suffices to prove that

$$2^N - 1 \,|\, 2^{2^N - 2} - 1. \tag{1.2}$$

We prove a stronger result, namely,

$$2^N - 1 \,|\, 2^{(2^N - 2)/2} - 1, \tag{1.3}$$

which implies (1.2). Noting that N is odd pseudoprime, we see that

$$\left(2^N - 2\right)/2 = 2^{N-1} - 1 = kN$$

for some integer k. Then

$$2^N - 1 \,|\, 2^{kN} - 1 = 2^{(2^N - 2)/2} - 1,$$

and (1.3) is satisfied. □

[KLS01, p.133] further notes that in 1903 this theorem was proved in [Mal03] for the case in which N is a prime and $2^N - 1$ is composite.

1.2.1 Even Pseudoprimes

A short note on even Pseudoprimes can be found in [Rib04, p.90**f**]: There also exist even composite integers satisfying the congruence $2^n \equiv 2 \pmod{n}$ - they may be called even pseudoprimes. The smallest one is $m = 2 \times 73 \times 1103 = 161038$, discovered by Lehmer in 1949 [Leh49].

1.2.2 Mersenne Numbers

According to [Chi09, p.209] and restating the introductory words in the beginning of this subsection "Mersenne numbers are at least plausible candidates for being primes, because they are always 2-pseudoprimes."

Proposition 1.5. *[Chi09, p.209] If n passes the 2-pseudoprime test, then $2^n - 1$ does also. Thus if n is prime, $2^n - 1$ is either prime or a 2-pseudoprime.*

Hint for proof. If $2^{n-1} - 1 = nq$, then $2^{(2^n-1)-1} - 1 = 2^{2^n-2} - 1 = (2^n)^{2q} - 1$, which has $2^n - 1$ as a factor. □

***Example* 1.6.** *[Chi09, p.209]* Fermat's theorem is of assistance in finding non-trivial factors of Mersenne numbers if they exist. For example, consider trying to factor $2^{37}-1$. Suppose p is a prime divisor of $2^{37} - 1$. Then $2^{37} \equiv 1 \pmod{p}$, and since 37 is prime, 37 must be the order of 2 modulo p. Thus by Fermat's theorem, 37 divides $p - 1$, that is, $p - 1 = 37k$ for some k. It follows that any prime divisor of $2^{37} - 1$ must be of the form $p = 1 + 37k$. Evidently we can assume that k is even, that is, p is a prime of the form $p = 1 + 74h$, for $h = 1,2,3,\ldots$
Such an analysis drastically reduces the number of trial divisions needed to decide whether or not $2^{37} - 1$ is prime. So we try:

$$\begin{aligned} h = 1, p = 75 \quad & \text{not prime;} \\ h = 2, p = 149 \quad & \text{prime, but not a divisor of } 2^{37} - 1; \\ h = 3, p = 223 \quad & \text{prime and a divisor of } 2^{37} - 1. \end{aligned}$$

Theorem 1.7. *[KLS01, p.44] All Mersenne number are primes or pseudoprimes to the base 2.*

Proof. Let $M_p = 2^p - 1$, where p is a prime, be a composite Mersenne number. Then p is an odd prime. It suffices to prove that

$$2^{M_p-1} \equiv 1 \pmod{M_p},$$

or equivalently,

$$M_p \mid 2^{M_p-1} - 1. \tag{1.4}$$

We prove a stronger result, namely,

$$M_p \mid 2^{(M_p-1)/2} - 1, \tag{1.5}$$

which implies (1.4). By Fermat's little theorem,

$$\frac{M_p - 1}{2} = 2^{p-1} - 1 \equiv 0 \pmod{p}.$$

Hence, $(M_p - 1)/2 = kp$ for some positive integer k. Noting that

$$2^p - 1 \mid 2^{kp} - 1,$$

we see that (1.5) holds. □

1.2.3 Fermat Numbers

As mentioned by [Chi09, p.209] F_n passes the 2-pseudoprime test for any n meaning the following.

Theorem 1.8. *[KLS01, p.36f] All Fermat numbers are primes or pseudoprimes to the base 2. Moreover, if $2^n + 1$ is a pseudoprime to the base 2, then n is a power of 2.*

Proof. Since $m \leq 2^m - 1$, we obtain from Lemma A.7.19 that

$$F_m \mid 2^{F_m} - 2.$$

Hence, each F_m is a prime or pseudoprime to the base 2 by Definition 1.2(b).
Suppose now that n is not a power of 2 and that $2^n + 1$ is a pseudoprime to the base 2. Then $2^n + 1$ is composite and

$$2^{2^n} \equiv 1 \pmod{2^n + 1}, \tag{1.6}$$

since $\gcd(2, 2^n + 1) = 1$. Note that

$$2^n \equiv -1 \pmod{2^n + 1}$$

and that $2^n < 2^n + 1$. Let $e = \operatorname{ord}_{2^n+1} 2$. Then $e \geq n + 1$, and by Lemma A.10.27, if $2^t \equiv 1 \pmod{2^n + 1}$, then $e \mid t$. Since

$$2^{2n} \equiv (-1)^2 \equiv 1 \pmod{2^n + 1},$$

it follows that $e = 2n$. Therefore, by (1.6) and Lemma A.10.27, we have $2n \mid 2^n$. However, this is impossible, since $2n$ is not a power of 2. □

1.3 Distribution and Infinitude

In the book of [Chi09, p.207] it is indicated that it turns out that 2-pseudoprimes are much less common than primes. How scarce are they? Here are some counts: There are 168 primes < 1000, but only three 2-pseudoprimes: $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, and $645 = 3 \cdot 5 \cdot 43$. There are 5,761,455 primes under 100,000,000, but only 2057 2-pseudoprimes. There are 882,206,716 primes less than $2 \cdot 10^{10}$, compared with 19,685 2-pseudoprimes less than $2 \cdot 10^{10}$ [PSW80]. Based on these counts and a comparison of the number of 2-pseudoprimes $< m$ with the number of primes $< m$ for large numbers m, it is evident that if you pick randomly a large number n and verify that n divides $2^{n-1} \equiv 1 \pmod{n}$, then it is highly probable that n is prime. For this reason, the mathematician Henri Cohen has called a number n with $2^{n-1} \equiv 1 \pmod{n}$ an "industrial grade prime ".

Nevertheless as written in [Rib04, p.90] it turns out, not surprisingly, that there are infinitely many pseudoprimes, and there are many ways to generate infinite sequences of pseudoprimes. The simplest proof was given in 1903 by Malo [Mal03], who showed the following theorem.

Theorem 1.9. *[Rib04, p.90] If n is a pseudoprime, and if $n' = 2^n - 1$, then n' is also a pseudoprime.*

Proof. Indeed, n' is obviously composite, because if $n = ab$ with $1 < a, b < n$, then

$$2^n - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Also n divides $2^{n-1} - 1$, hence n divides $2^n - 2 = n' - 1$; so $n' = 2^n - 1$ divides $2^{n'-1} - 1$. □

Another way of proving infinitude of Poulet numbers is shown in [KLS01, p.131-132]. As pointed out in the previous subsection, there are interesting connections between Fermat numbers and pseudoprimes. It was proved in Theorem 1.8 that all composite Fermat numbers are pseudoprimes. If there are infinitely many composite Fermat numbers, then this would show that there are infinitely many pseudoprimes. Unfortunately, it is not known whether or not there are infinitely many composite Fermat numbers. On the other hand, as we will see, Fermat numbers have been used by several authors (see [Cip04], [Jar50], [Jea98], [Rot64], [Szy66]) to generate infinitely many pseudoprimes. Although pseudoprimes resemble primes by being infinite in number and by satisfying the assertion of Fermat's little Theorem, they also differ strikingly from primes in various ways.

The following theorem, proved in [Cip04] in 1904, shows how Fermat numbers can be used to generate infinitely many pseudoprimes, including pseudoprimes with an arbitrary number of prime factors.

Theorem 1.10. ***(Cipolla)*** *[KLS01, p.132] If $a > b > \cdots > s > 1$ and $N = F_a F_b \cdots F_s$, then N is a pseudoprime if and only if $2^s > a$. In particular, given any positive integer M, no matter how large, there exist infinitely many pseudoprimes with at least M distinct prime factors.*

Proof. Since $\gcd(F_m, F_n) = 1$ if $m \neq n$ by Goldbach's Theorem A.7.20, it is easy to see that

$$\operatorname{ord}_N 2 = \operatorname{lcm}\left(\operatorname{ord}_{F_a} 2, \operatorname{ord}_{F_b} 2, \ldots, \operatorname{ord}_{F_s} 2\right).$$

By Remark A.7.22, $\operatorname{ord}_{F_m} 2 = 2^{m+1}$ for $m \geq 0$. Thus,

$$\operatorname{ord}_N 2 = \operatorname{lcm}\left(2^{a+1}, 2^{b+1}, \ldots, 2^{s+1}\right) = 2^{a+1}.$$

Therefore, $2^{N-1} \equiv 1 \pmod N$ if and only if $N - 1$ is divisible by 2^{a+1}. However,

$$N - 1 = F_a F_b \cdots F_s - 1 = 2^{2^s} K,$$

where K is an odd integer. Hence, N is a pseudoprime if and only if $2^s > a$.
Now let $s > 1$ and let

$$N = F_s F_{s+1} F_{s+2} \cdots F_{2^s - 1}. \tag{1.7}$$

Then N is a pseudoprime by our above arguments. Clearly, given the positive integer M, we can choose s such that $2^s - s \geq M$ distinct prime factors. The theorem is thus proved. □

***Remark* 1.11.** *[KLS01, p.132f]*

(i) We note that the method given in Theorem 1.10 can be used to generate pairwise coprime pseudoprimes. Let the pseudoprimes N_1 and N_2 each be the product of distinct Fermat numbers such that no Fermat number appearing in N_1 appears in N_2. Since $\gcd(F_m, F_n) = 1$ for $m \neq n$, we see that N_1 and N_2 are coprime. We also note that it was shown in [Erd49] that for every $M \geq 2$ there exist infinitely many pseudoprimes that are the product of exactly M distinct primes.

(ii) It is of interest that the first proof of the infinitude of pseudoprimes appears in [Jea98] in 1898 and also makes use of Fermat numbers. Specifically, Jeans showed that if $a > b$ and $2^b > a$, then $F_a F_b$ is a pseudoprime. This result is a special case of Theorem 1.10.

Further in [Rib04, p.90*f*] it is noted, that Fermat numbers are pairwise relatively prime, so the above method leads to pairwise relatively prime pseudoprimes. One can also obtain pseudoprimes having an arbitrarily large number of prime factors.

In 1936, Lehmer [Leh36] found a very simple method to generate infinitely many pseudoprimes, each one being the product of two distinct primes p, q. Namely, let $k \geq 5$ be an arbitrary odd integer, let p be a primitive prime factor of $2^k - 1$, and let q be a primitive prime factor of $2^k + 1$. Then pq is a pseudoprime. Thus, for every $m \geq 1$ there exist at least m pseudoprimes $n = pq$ such that

$$n \leq \left(2^{2m+3} - 1\right)\left(\frac{2^{2m+3}+1}{3}\right) = \frac{4^{2m+3}-1}{3}.$$

***Remark* 1.12.**

(i) *[KLS01, p.133]* Theorem 1.4 shows in another way, different form Cipolla's Theorem 1.10, that there exist infinitely many pseudoprimes. By Theorem 1.8 we know that if F_m is composite, then F_m is a pseudoprime. From Theorem 1.4 it follows that for each pseudoprime we can find a greater one. Thus, the set of pseudoprimes is unbounded and hence infinite.

(ii) *[KLS01, p.133]* Theorem 1.4, which appears in [Sie47] and [Ste48], can be used to recursively generate infinitely many pseudoprimes for a given composite Fermat number.

Now following [KLS01, p.133] the next Theorem, from [Rot64], also uses Fermat numbers to generate infinitely many pseudoprimes and bears a certain resemblance to Theorem 1.10. This Theorem generalizes Theorem 1.4 as well in the case for which N is a Fermat number.

Theorem 1.13. *[KLS01, p.133] (**Rotkiewicz**) If $n_1 > n_2 > \cdots n_s > 1$, $s > 1$, $2^{n_s} > n_1$, and*

$$N = \left(2^{F_{n_1}} - 1\right)\left(2^{F_{n_2}} - 1\right)\cdots\left(2^{F_{n_s}} - 1\right),$$

then N is a pseudoprime. In particular, given any positive integer M, no matter how large, there exist infinitely many pseudoprimes with a least M distinct prime factors.

For proving Theorem 1.13, but before we will need Lemma 1.14 (c.f. [KLS01, eq. (9.11), (11.3), Lemma 6.3]).

Lemma 1.14. *[KLS01, p.134] Let a and b be coprime integers with $|a| > |b| \geq 1$ and let m and n be positive integers. Then*

$$\gcd\left(a^m - b^m, a^n - b^n\right) = \left|a^{\gcd(m,n)} - b^{\gcd(m,n)}\right|. \tag{1.8}$$

For a *proof* of the equality

$$\gcd\left(\frac{a^m - b^m}{a-b}, \frac{a^n - b^n}{a-b}\right) = \left|\frac{a^{\gcd(m,n)} - b^{\gcd(m,n)}}{a-b}\right|,$$

which is equivalent to (1.8), see [Car13, p. 38] or [Wil98, p. 87].

Proof of Theorem 1.13. Let $d_i = 2^{F_{n_i}} - 1$ for $1 \leq i \leq s$. To prove that N is a pseudoprime, it suffices to show that $\mathrm{ord}_N 2 \,|\, N-1$. Since $\gcd(F_{n_i}, F_{n_j}) = 1$ for $1 \leq i < j \leq s$ by Goldbach's Theorem A.7.20, it follows by Lemma 1.14 that $\gcd(d_i, d_j) = 1$ if $1 \leq i < j \leq s$. Thus,

$$\mathrm{ord}_N 2 = \mathrm{lcm}(\mathrm{ord}_{d_1} 2, \mathrm{ord}_{d_2} 2, \ldots, \mathrm{ord}_{d_s} 2). \tag{1.9}$$

Clearly, the order of 2 modulo $2^{F_{n_i}} - 1$ is equal to F_{n_i} for $1 \leq i \leq s$. Hence, by (1.9),

$$\mathrm{ord}_N 2 = \mathrm{lcm}(F_{n_1}, F_{n_2}, \ldots, F_{n_s}) = F_{n_1} F_{n_2} \cdots F_{n_s}.$$

We now note that

$$N - 1 = \left(2^{F_{n_1}} - 1\right)\left(2^{F_{n_2}} - 1\right) \cdots \left(2^{F_{n_s}} - 1\right) - 1. \tag{1.10}$$

Since $\mathrm{ord}_{F_m} 2 = 2^{m+1}$ by Remark A.7.21 and since $2^{n_s} > n_1$, it follows that

$$2^{F_{n_i} - 1} \equiv 1 \pmod{F_{n_j}}$$

for any i and j such that $1 \leq i, j \leq s$. Hence,

$$2^{F_{n_i}} - 1 \equiv 2 - 1 \equiv 1 \pmod{F_{n_j}} \tag{1.11}$$

for $1 \leq i, j \leq s$. By (1.10) and (1.11), we see that

$$N - 1 \equiv 1 \cdot 1 \cdots 1 - 1 \equiv 0 \pmod{F_{n_i}}$$

for $1 \leq i, j \leq s$. Hence,

$$N - 1 \equiv 0 \pmod{F_{n_1} F_{n_2} \cdots F_{n_s}}$$

and $\mathrm{ord}_N 2 \,|\, N - 1$. The rest of the theorem follows by the same arguments as in proof of Cipolla's Theorem 1.10. □

Somehow more detailed statements on distribution are given in [KLS01, p.135]. Even though pseudoprimes are infinite in number, they are much scarcer than primes. For example, it was first proved in [Szy67] that if P_n denotes the n^{th} pseudoprime to the base 2, then

$$\sum_{n=1}^{\infty} \frac{1}{P_n}$$

is convergent, whereas it is well known that if p_n denotes the n^{th} prime, then

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

is divergent. However, in [Mąk74] it was shown that the series below is divergent.

$$\sum_{n=1}^{\infty} \frac{1}{\log P_n}$$

As defined in [Rib04, p.217] let $P\pi(x) = |\{n|1 \leq n \leq x$, n is 2-pseudoprime$\}|$. For the upper bound of $P\pi(x)$, improving on a previous result of Erdös (1956) [Erd56], Pomerance showed in 1981 [Pom81], that for all large x,

$$P\pi(x) \leq \frac{x}{\ell(x)^{1/2}}, \quad \text{with} \quad \ell(x) = \exp(\log x \log\log\log x / \log\log x).$$

Using the method of Lehmer to generate pseudoprimes to the base 2, which is elementary, it is possible to obtain the explicit, but weaker lower bound $0.171 \log x \leq P\pi(x)$. The tables of pseudoprimes suggest that for every $x \geq 170$ there exists a pseudoprime between x and $2x$. However, this has not yet been proved. In this direction, I note the following results of Rotkiewicz (1965) [Rot65]:

Theorem 1.15. *(**Rotkiewicz**) [Rib04, p.217]*
If n is an integer, $n > 19$, there exists a pseudoprime between n and n^2. Also, for every $\varepsilon > 0$ there exists $x_0 = x_0(\varepsilon) > 0$ such that, if $x > x_0$, then there exists a pseudoprime between x and $x^{1+\varepsilon}$.

Taking a look on the special set of even pseudoprimes (Poulet numbers) it can be found in [Rib04, p.90*f*] that in 1951, Beeger [Bee51] showed the existence of infinitely many even pseudoprimes; each one must have at least two odd prime factors. In addition to this [Sie88, p.230*ff*] indicates that later A. Rotkiewicz [Rot59a] has proved that the following assertion is also true. *For arbitrary natural numbers a and b there exist infinitely many even numbers n such that $n|a^n b - ab^n$.* This in turn, implies that for every natural number a there exist infinitely many even numbers n such that $n|a^n - a$. A. Rotkiewicz [Rot63, Rot67] has proved that there exists infinitely many pseudoprime numbers of the form $ax + b$ (x = 0,1,2, ...), where a, b are relatively prime integers; $a > 0$ (see also Rotkiewicz [Rot72]).

Theorem 1.16. *(**Rotkiewicz**) [KLS01, p.139]*
If $a \geq 1$, $d \geq 1$, and $\gcd(a, d) = 1$, then there exist infinitely many pseudoprimes in the arithmetic progression $\{a + kd|k \geq 1\}$.

Again in [Rib04, p.90*f*] it is asked how "far" are pseudoprimes from being primes? From Cipolla's result, there are pseudoprimes with arbitrarily many prime factors. This is not an accident. In fact, in 1949 Erdös [Erd49] proved that for every $k \geq 2$ there exist infinitely many pseudoprimes, which are the product of exactly k distinct primes.

2 Fermat Pseudoprimes

As said in [Rib04, p.92*ff*] it is also useful to consider the congruence $a^{n-1} \equiv 1 \pmod{n}$, for $a > 2$. If n is a prime and $1 < a < n$, then the above congruence holds necessarily. So, if, for example, $2^{n-1} \equiv 1 \pmod{n}$, but, say, $3^{n-1} \not\equiv 1 \pmod{n}$, then n is not a prime.

In the contrapositive point of view Fermat's little Theorem says if there exists a such that $1 < a < n$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite, but not conversely. This gives therefore a very practical way to ascertain that many numbers are composite.

Or even more specific written in [Chi09, p.210]: If we want to see if a number m is prime using trial division, we would not test m by just dividing by 2 - we would try dividing m by many primes. Similarly, there is no reason to test a number n for primeness by using just the 2-pseudoprime test. Fermat's theorem states that if a is any number not a multiple of m, and m is prime, then $a^{m-1} - 1$ is divisible by m. Thus instead of checking to see if $2^{m-1} \equiv 1 \pmod{m}$, we could pick any number $a < m$ and see if $a^{m-1} \equiv 1 \pmod{m}$. As adumbrated in section 1 this compositeness test based on Fermat's little Theorem is called the **a-pseudoprime test**.
If m fails an a-pseudoprime test, that is, if

$$a^{m-1} \not\equiv 1 \pmod{m},$$

for a single number $a < m$, then m is composite.
According to [Rib04, p.92] this leads to the more general study of pseudoprimes in an arbitrary base a.

2.1 Definition

Definition 2.1.

(Version a) as in *[FR07, p.218], [Chi09, p.210], [Rie94, p.86], [Guy04, p.27]*
Let n be a(n odd) composite integer. If $a > 1$ with $\gcd(n, a) = 1$ and $a^{n-1} \equiv 1 \pmod{m}$ then n is called an *a-pseudoprime* (or also called *Fermat pseudoprime for base a* or sometimes denoted by $\mathrm{psp}(a)$).

(Version b) as in *[KLS01, p.36], [CP05, p.132]*
A composite number n such that $n \mid a^n - a$ is called a *(Fermat) pseudoprime* to the base a.

***Remark* 2.2.**

(i) *[KLS01, p.131]* According to definition 2.1(b), a composite integer n is called a pseudoprime to the base a if (A.11) holds. If $\gcd(a, n) > 1$, then (A.12) is not satisfied, but (A.11) may be satisfied. Sometimes the notion of pseudoprimes like in definition 2.1(a) is based on congruence (A.12) in contrast to the congruence given in (A.11), and so produces a *smaller class of composite numbers* satisfying the converse Fermat's little Theorem A.5.10.

(ii) *[Rie94, p.86]* The term pseudoprime has been used in older literature for *any* n satisfying (A.12), primes as well as composites, thus including both primes and false primes! In more modern texts the term "probable prime" (PRP) is often used for prime number candidates until their primality (or compositeness) has been established.

(iii) *[FR07, p.218]* Hence n is a pseudoprime to the base a if it passes the Fermat test and hence is a *probable prime*.

(iv) *[Guy04, p.44]* Pomerance, Selfridge & Wagstaff call an odd composite n for which $a^{n-1} \equiv 1 \pmod{n}$ a **pseudoprime to base** a (psp(a)). This usage is introduced to avoid the clumsy "composite pseudoprime" which appears throughout the literature.

In [Rie94, p.86*f*] it is stated that now, if all the pseudoprimes for some particular base were known, then a Fermat test performed for this base in combination with a list of pseudoprimes would actually constitute a fast primality test. As a matter of fact this works very well for numbers of limited size! The technique has been made use of by D.H. Lehmer, (see [Leh36, Leh49]), who prepared a list of all Fermat pseudoprimes below $2 \cdot 10^8$ for base 2 with no factor > 317. Lehmer's list of pseudoprimes starts at 10^7 which was the limit of the existing prime tables at the time. In order to test a number N between 10^7 and $2 \cdot 10^8$ for primality with aid of Lehmer's list this scheme was followed:

1. Perform trial division by the 65 primes ≤ 313. If a divisor is found N is composite.
2. Compute $2^{N-1} \pmod{N}$. If the residue is $\not\equiv 1$, then N is composite.
3. For the residue 1, check with Lehmer's list of pseudoprimes. If N is in the list, it is composite and its factors are given in the list. If not in the list, N is a prime.

About 15 years ago this technique of settling the question of primality for numbers of limited size has been pushed further by Carl Pomerance, John Selfridge and Samuel Wagstaff and is reported in [PSW80]. It appeared that below $25 \cdot 10^9$ there are 21853

pseudoprimes for base 2, of which 4709 remain if base 3 is also tested. Of these, base 5 leaves 2552 and, finally, base 7 eliminates all but 1770. Thus if a list is available of these 1770 numbers below $25 \cdot 10^9$, the pseudoprimes for all four bases 2, 3, 5 and 7, we can decide upon the primality of any number up to this limit by performing at most four Fermat tests. Fermat tests are computationally fast. One Fermat test can, as a matter of fact, be carried out in at most $2\log_2 N$ steps, each step consisting of the multiplication and reduction $\bmod N$.

2.2 Properties

Lemma 2.3. *[FR07, p.219] If n is a pseudoprime to the base b_1 and also a pseudoprime to the base b_2 and $\gcd(b_1, b_2) = 1$, then it is a pseudoprime to the base $b_1 b_2$.*

***Remark* 2.4.** *[FR07, p.219]* Probabilistic methods proceed by testing n to a base b_1. If it is not a pseudoprime then it is composite and we are done. If it is a pseudoprime, test a second base b_2 and so on, in the hope of finding a base for which n is not a pseudoprime. However, there do exist numbers which are pseudoprimes to every possible base, as we will see in section 3.

Theorem 2.5. *[KLS01, p.47] Let $m \geq 5$ and let $F_m = FC$, where $F > 1$ and $C > 1$. If*

$$3^{F-1} \not\equiv 3^{F_m-1} \pmod{C},$$

then C is composite. If

$$3^{F-1} \equiv 3^{F_m-1} \pmod{C},$$

then C is a pseudoprime to the base 3^F or a prime.

Proof. We first show that if C is prime, then

$$3^{F-1} \equiv 3^{F_m-1} \pmod{C}.$$

According to Goldbach's Theorem A.7.20, $\gcd(3, F_m) = 1$. Now it follows, by Fermat's little theorem A.5.10, that

$$3^{F-1} \equiv \left(3^{F-1}\right)^C \equiv 3^{FC-C} \equiv \frac{3^{FC}}{3^C} \equiv \frac{3^{FC}}{3} \equiv 3^{FC-1} \equiv 3^{F_m-1} \pmod{C}.$$

Now suppose that

$$3^{F_m-1} = 3^{FC-1} \equiv 3^{F-1} \pmod{C}. \tag{2.1}$$

Noting that $\gcd(3^{F-1}, F_m) = \gcd(3^{F-1}, C) = 1$, we can cancel out 3^{F-1} in congruence (2.1) to obtain

$$3^{FC-F} = 3^{F(C-1)} = (3^F)^{C-1} \equiv 1 \pmod{C},$$

which implies that C is a pseudoprime to the base 3^F or a prime. □

Another interesting property of Fermat pseudoprimes is outlined in [Rib04, p.94]. It may occur that a number is a pseudoprime for different bases, like 561 for the bases 2, 5, 7. Indeed, Baillie & Wagstaff [BW80] and Monier [Mon80] showed independently, in 1980, the following result: Let n be a composite number, and let $B_{\text{psp}}(n)$ be the number of bases a, $1 < a < n$, with $\gcd(a, n) = 1$, for which n is an $a-$pseudoprime. Then

$$B_{\text{psp}}(n) = \left\{ \prod_{p|n} \gcd(n-1, p-1) \right\} - 1$$

It follows that if n is an odd composite number, which is not a power of 3, then n is a pseudoprime for at least two bases a, $1 < a \leq n-1$.

2.3 Distribution and Infinitude

In [Chi09, p.210] the following indications on the distribution of Fermat Pseudoprimes are given. We observed that 2-pseudoprimes are fairly rare, and the same is true for a-pseudoprimes for any a. So it is plausible that numbers that are simultaneously 2- and 3-pseudoprimes are rarer still.

***Example* 2.6.** *[Chi09, p.210]* For example, neither of the 2-pseudoprimes 341 and 645 is a 3-pseudoprime: the latter because 3 divides 645. Neither is 1194649, the 2-pseudoprime we found between 1194601 and 1194700. In fact,

$$3^{194648} \equiv 341017 \pmod{1194649}$$

so 1194649 is not prime because it fails the 3-pseudoprime test.

Continuing with [Chi09, p.210f] more systematically, we could treat Fermat's theorem like trial division: take a number m, and check to see if

$$a^{m-1} \equiv 1 \pmod{m}$$

for many numbers a. Very few numbers would pass these a-pseudoprime tests and not be prime. Evidently, numbers that are a-pseudoprimes for more than one number a are uncommon.

For the proof of infinitude [CP05, p.132] discusses the following theorem 2.7. For pseudoprimes defined via the congruence (A.12), this theorem was first proved in [Erd50]. For the possibly larger class of pseudoprimes defined via (A.11) the theorem was first proved in [Li97].
Theorem 2.7 tells us that using the Fermat congruence to distinguish between primes

and composites is potentially very useful. However, this was known as a practical matter long before the Erdös proof.

Theorem 2.7. *[CP05, p.132] For each fixed integer $a \geq 2$, the number of Fermat pseudoprimes base a that are less than or equal to x is $o(\pi(x))$ as $x \to \infty$. That is, Fermat pseudoprimes are rare compared with primes.*

Furthermore [CP05, p.132] notes that odd numbers n satisfy (A.12) for $a = n-1$, so that the congruence does not say very much about n in this case. If (A.12) holds for a pair n, a, where $1 < a < n-1$, we say that n is a **probable prime** base a. Thus, if n is a prime, then it is a probable prime base a for every integer a with $1 < a < n-1$. Theorem 2.7 asserts that for a fixed choice of a, most probable primes base a are actually primes. We thus have a simple test to distinguish between members of a set that contains a sparse set of composite numbers and all of the primes exceeding $a+1$, and members of the set of the remaining composite numbers exceeding $a+1$.
We have seen that with respect to a fixed base a, pseudoprimes (that is, probable primes that are composite) are sparsely distributed. However, paucity notwithstanding, there are infinitely many.

Theorem 2.8. *[CP05, p.133] For each integer $a \geq 2$ there are infinitely many Fermat pseudoprimes base a.*

Proof. We shall show that if p is any odd prime not dividing a^2-1, then $n = (a^{2p}-1)/(a^2-1)$ is a pseudoprime base a. For example, if $a = 2$ and $p = 5$, then this formula gives $n = 341$. First note that

$$n = \frac{a^p - 1}{a-1} \cdot \frac{a^p + 1}{a+1}$$

so that n is composite. Using (A.11) for the prime p we get upon squaring both sides that $a^{2p} \equiv a^2 \pmod{p}$. So p divides $a^{2p} - a^2$. Since p does not divide $a^2 - 1$, by hypothesis, and since $n - 1 = (a^{2p} - a^2)/(a^2 - 1)$, we conclude that p divides $n - 1$. We can conclude a second fact about $n - 1$ as well: Using the identity

$$n - 1 = a^{2p-2} + a^{2p-4} + \cdots + a^2, \tag{2.2}$$

we see that $n - 1$ is the sum of an even number of terms of the same parity, so $n - 1$ must be even. So far, we have learned that both 2 and p are divisors of $n - 1$, so that $2p$ must likewise be a divisor. Then $a^{2p} - 1$ is a divisor of $a^{n-1} - 1$. But $a^{2p} - 1$ is a multiple of n, so that (A.12) holds, as does (A.11). □

Different options to prove $a-$pseudoprimes' infinitude are shown in [Rib04, p.92]. In 1904, Cipolla [Cip04] also indicated how to obtain $a-$pseudoprimes. Let $a \geq 2$, let p

be any odd prime such that p does not divide $a(a^2-1)$. Let

$$n_1 = \frac{a^p-1}{a-1}, \qquad n_2 = \frac{a^p+1}{a+1}, \qquad n = n_1 n_2;$$

then n_1 and n_2 are odd and n is composite. Since $n_1 \equiv 1 \pmod{2^p}$ and $n_2 \equiv 1 \pmod{2^p}$, then $n \equiv 1 \pmod{2^p}$. From $a^{2p} \equiv 1 \pmod{n}$ it follows that $a^{n-1} \equiv 1 \pmod{n}$, so n is an $a-$pseudoprime. Since there exist infinitely many primes, then there also exist infinitely many a-pseudoprimes (also when $a > 2$).

There are other methods in the literature to produce very quickly increasing sequences of a-pseudoprimes. For example, Crocker [Cro62] proceeded as follows in 1962. Let a be even, but not of the form 2^{2^r} , with $r \geq 0$. Then, for every $n \geq 1$, the number $a^{a^n}+1$ is an $a-$pseudoprime. In 1948, Steuerwald [Ste48] established the following infinite sequence of $a-$pseudoprimes. Let n be an $a-$pseudoprime, which is prime to $a-1$. For example, for a prime q, put $a = q+1$ and let p be a prime such that $p > a^2-1$; as in the Cipolla construction, let

$$\begin{aligned} n_1 &= \frac{a^p-1}{a-1} \equiv a^{p-1} + a^{p-2} + \cdots + a + 1 \equiv p \pmod{q}, \\ n_2 &= \frac{a^p+1}{a+1} \equiv a^{p-1} - a^{p-2} + \cdots - a + 1 \equiv 1 \pmod{q}, \end{aligned}$$

so $n = n_1 n_2 \equiv p \pmod{q}$. Let now $f(n) = (a^n-1)/(a-1) > n$. Then $f(n)$ is also an $a-$pseudoprime. Indeed,

$$f(n) = \frac{a^{n_1 n_2}-1}{a^{n_2}-1} \times \frac{a^{n_2}-1}{a-1}$$

is composite. Since n is prime to $a-1$ and $a^{n-1} \equiv 1 \pmod{n}$, then n divides $(a^n - a)/(a-1) = f(n)-1$. Thus $f(n)$ divides a^n-1, which divides $a^{f(n)-1}-1$, hence $f(n)$ is an $a-$pseudoprime. The process may be iterated, noting that $f(n)$ is prime to $a-1$:

$$\begin{aligned} f(n) &= \frac{[(a-1)+1]^n - 1}{a-1} \\ &= (a-1)^{n-1} + \binom{n}{1}(a-1)^{n-2} + \cdots + \binom{n}{n-2}(a-1) + n \\ &\equiv n \pmod{a-1} \end{aligned}$$

so $f(n)$ is an $a-$pseudoprime that is prime to $a-1$. This process leads to an infinite increasing sequence of $a-$pseudoprimes $n < f(n) < f(f(n)) < f(f(f(n))) < \ldots$, which grows as $n, a^n, a^{a^n} a^{a^{a^n}}, \ldots$ The method of Lehmer indicated above, applied to binomials a^k-1 and a^k+1, produces $a-$pseudoprimes which are the product of two distinct prime factors. From these considerations it follows that it is futile to wish to discover the largest $a-$pseudoprime.

In 1958, Schinzel [Sch58] showed that for every $a \geq 2$, there exist infinitely many pseudoprimes in base a that are products of two distinct primes. In 1971, in his thesis, Lieuwens [Lie71] extended simultaneously this result of Schinzel and Erdös' result about pseudoprimes in base 2: for every $k \geq 2$ and $a > 1$, there exist infinitely many pseudoprimes in base a, which are products of exactly k distinct primes. In 1972, Rotkiewicz [Rot72] showed that if $p \geq 2$ is a prime not dividing $a \geq 2$, then there exist infinitely many pseudoprimes in base a that are multiples of p; the special case when $p = 2$ dates back to 1959, also by Rotkiewicz [Rot59b].

3 Carmichael Numbers

As seen in the previous section there exist Fermat pseudoprimes, which are a-pseudoprimes for different bases a. As mentioned in [Rib04, 100] in a short article, which remained unnoticed, Korselt [Kor99] considered in 1899 a more rare kind of numbers; they were also introduced independently by Carmichael in 1912 [Car12], who first studied their properties. Since his article was noted, such numbers came to be called Carmichael numbers.
In [CP05, p.133] the problem of those Carmichael numbers referring to primality tests is adumbrated. In search of a simple and quick method of distinguishing prime numbers from composite numbers, we might consider combining Fermat tests for various bases a. For example, though 341 is a pseudoprime base 2, it is not a pseudoprime base 3. And 91 is a base-3, but not a base-2 pseudoprime. Perhaps there are no composites that are simultaneously pseudoprimes base 2 and 3, or if such composites exist, perhaps there is some finite set of bases such that there are no pseudoprimes to all the bases in the set. It would be nice if this were true, since then it would be a simple computational matter to test for primes. However, the number $561 = 3 \cdot 11 \cdot 17$ is not only a Fermat pseudoprime to both bases 2 and 3, it is a pseudoprime to every base a. It may be a shock that such numbers exist, but indeed they do.
In addition [Rie94, p.87] indicates a Carmichael number never reveals its compositeness under a Fermat test, unless a happens to be a divisor of N, a situation which can be avoided by first testing whether $\gcd(a, N) > 1$. Although the Carmichael numbers are rather scarce, there do exist enough of them to create frustration when a number of Fermat tests all yield the result $a^{N-1} \equiv 1 \pmod{N}$.

3.1 Definition

There is also some confusion in literature concerning notation and definition, of course caused by different definitions of Fermat pseudoprimes. Regarding Carmichael numbers the term *absolute pseudoprime* is sometimes used likewise as seen in [KLS01, p.135]. A more distinct definition was given and discussed by [Sie88, p.232f].

Definition 3.1. *[Sie88, p.232]* A composite number n is called an *absolutely pseudoprime number* if for every integer a number $a^n - a$ is divisible by n.

As noted in [Sie88, p.233] if n is an absolutely pseudoprime number and a is an integer relatively prime to n, then, since $a^n - a = a(a^{n-1} - 1)$ is divisible by n, number $a^{n-1} - 1$ must be divisible by n.

Definition 3.2. *[Sie88, p.233]* Composite numbers n such that $n | a^{n-1} - 1$ holds if $\gcd(a, n) = 1$ are called *Carmichael numbers*.

[Sie88, p.233] proceeds to declare Carmichael was the first to notice the existence of these numbers in 1909 [Car10]. We see that any absolutely pseudoprime number is a Carmichael number. It can be proved that the converse is also true.
Other authors do not distinguish between the notations, or even do not refer to the notation "absolute pseudoprime" . In [CP05, p.211], [Rib04, p.100], and [Rie94, p.87] there are only mentioned Carmichael numbers and they define them like in [Sie88, p.233]. It can be seen in [FR07, p.219] and [Chi09, p.211] that some authors define Carmichael number by being simply Fermat pseudoprimes for any base a.
Now an acquainted example of Carmichael numbers should be noted, namely the smallest one.

***Example* 3.3.** *[Chi09, p.211]* Show that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.
First note that $561 = 3 \cdot 11 \cdot 17$ is composite. We want to show that for any a coprime to 561, $a^{560} \equiv 1 \pmod{561}$. To do so, suffices to show that

$$\begin{aligned} a^{560} &\equiv 1 \pmod 3, \\ a^{560} &\equiv 1 \pmod{11}, \text{ and} \\ a^{560} &\equiv 1 \pmod{17}. \end{aligned}$$

Now by Fermat's theorem, $a^2 \equiv 1 \pmod 3$, $a^{10} \equiv 1 \pmod{11}$ and $a^{16} \equiv 1 \pmod{17}$ for every number a coprime to 3, 11, and 17. Since 560 is a multiple of 2, 10, and 16, it follows that each of the displayed congruences is true.

[Rib04, p.219f] refers more extensively to tables of pseudoprimes and of Carmichael numbers. In 1938 Poulet [Pou38] determined all the (odd) pseudoprimes (in base 2) up to 10^8. Carmichael numbers were starred in Poulet's table. In 1975, Swift [Swi75] compiled a table of Carmichael numbers up to 10^9, while in 1979 Yorinaga [Yor79] went up to 10^{10}. The table of Pomerance, Selfridge & Wagstaff (1980) [PSW80] comprises pseudoprimes, Euler pseudoprimes, strong pseudoprimes (in base 2) and Carmichael numbers and goes to 25×10^9. It was extended by Pinch to 10^{12} in 1992 and to 10^{13} in 2000 [Pin92, Pin00].
In 1990, Jaeschke [Jae90] extended the table of Carmichael numbers up to 10^{12}. It was further extended (and slightly amended) by Pinch to 10^{15} in 1993 and to 10^{16} in 1998 [Pin93, Pin98]. Pinch has also published other tables about Carmichael numbers:

(1) List of the smallest Carmichael number having k prime factors, for $3 \leq k \leq 20$.

(2) Number of Carmichael numbers in the residue classes modulo 5, 7, 11, 12, up to 25×10^9 and also up to 10^M for $11 \leq M \leq 16$.

(3) Frequency of each prime $p \leq 97$ as a factor (resp. as the smallest factor) of a Carmichael number, up to the bounds just indicated.

3.2 Properties

[FR07, p.219] states that the Carmichael numbers can be completely classified. Interestingly, this was done even before the existence of Carmichael numbers was shown. The first characterization of Carmichael numbers has been done by A. Korselt in 1899 [Kor99].

Theorem 3.4. *(**Korselt's Criterion**) [Chi09, p.414]*
An odd composite number m is a Carmichael number if and only if m is square-free and $(p-1)|(m-1)$ for every prime p dividing m.

Proof. Suppose m is square-free and $p-1$ divides $m-1$ for all primes p dividing m. Let b be coprime to m. Then for all p dividing m, b is coprime to p, so $b^{m-1} \equiv 1 \pmod{p}$ by Fermat's theorem. Since $p-1$ divides $m-1$, $b^{m-1} \equiv 1 \pmod{p}$. Now since m is square-free, m is the least common multiple of the primes which divide m. So if $b^{m-1} \equiv 1 \pmod{p}$ for all p dividing m, then $b^{m-1} \equiv 1 \pmod{m}$. So m is Carmichael. Conversely, suppose m is Carmichael, and suppose p is any (odd) prime divisor of m. Let $m = p^e q$, where $\gcd(p, q) = 1$. Let b be a primitive root modulo p^e, and let a be a number such that

$$\begin{aligned} a &\equiv b \pmod{p^e} \\ a &\equiv 1 \pmod{q} \end{aligned}$$

Then a is coprime to m. If m is Carmichael, then

$$\begin{aligned} a^{m-1} &\equiv 1 \pmod{m} \\ \text{so} \quad a^{m-1} &\equiv 1 \pmod{p^e}. \end{aligned}$$

But the order of a modulo p^e is $p^e(p-1)$. So $p^{e-1}(p-1)$ divides $m-1$, and hence $p-1$ divides $m-1$. Also, if $e > 1$, then p divides $m-1$. But since p divides m, p cannot divide $m-1$. Thus $e = 1$. Since this is true for all primes p dividing m, therefore m must be square-free. □

***Example* 3.5.** *[Chi09, p.414]* Korselt's criterion is quite useful for identifying Carmichael numbers. By theorem 3.4 2821 is Carmichael: 2821 factors as $7 \cdot 13 \cdot 31$, and 2820 is divisible by 6, 12 and 30: in fact, $2820 = 12 \cdot 235 = 30 \cdot 94 = 6 \cdot 470$.

An annotation in [KLS01, p.136] says that in 1910, Carmichael [Car10] independently discovered Korselt's criterion above and reformulated it in the following manner using the Carmichael lambda function defined in A.6.12.

Theorem 3.6. *[KLS01, p.136] A composite integer N is a Carmichael number if and only if N is square-free and $\lambda(N) \mid N-1$, where λ is the Carmichael lambda function.*

***Remark* 3.7.** *[KLS01, p.136]* In this paper, Carmichael also showed that a Carmichael number has at least three prime divisors and gave examples of four Carmichael numbers including the smallest such numbers, 561 and 1105. In [Car12] fifteen Carmichael numbers were given.

Corollary 3.8. *[FR07, p.220]*
A Carmichael number must be divisible by at least three primes.

Proof. Suppose that n is a Carmichael number. Then from the proof of the previous theorem, $n = p_1 \cdots p_k$ with $k \geq 2$ and the p_i distinct primes. We must show that $k > 2$. Suppose that $n = pq$ with $p < q$ primes. Since n is a Carmichael number, from the previous theorem $(q-1)|(n-1)$. However,

$$n - 1 = pq - 1 = p(q - 1 + 1) - 1 \equiv p - 1 \pmod{q-1}. \tag{3.1}$$

Since $(q-1)|(n-1)$ this would imply that $(q-1)|(p-1)$, which is impossible since $p < q$. Therefore if $n = pq$ it cannot be a Carmichael number and hence $k > 2$, so that n must be divisible by at least three distinct primes. □

In [Rib04, p.101] it is written that in 1939, Chernick [Che39] gave the following method to obtain Carmichael numbers. Let $m \geq 1$ and

$$M_3(m) = (6m + 1)(12m + 1)(18m + 1).$$

If m is such that all three factors above are prime, then $M_3(m)$ is a Carmichael number. This yields Carmichael numbers with three prime factors. Similarly, if $k \geq 4$, $m \geq 1$, let

$$M_k(m) = (6m + 1)(12m + 1)\prod_{i=1}^{k-2}(9 \times 2^i m + 1).$$

If m is such that all k factors are prime numbers and, moreover, 2^{k-4} divides m, then $M_k(m)$ is a Carmichael number with k prime factors.

Proposition 3.9. *[Chi09, p.414f]*
Let $m = (6k+1)(12k+1)(18k+1)$. Then m is Carmichael for all k for which all three factors of m are prime.

Proof. Observe that

$$\begin{aligned} m &= (6k + 1)(12k + 1)(18k + 1) = 1296k^3 + 393k^2 + 36k + 1 \\ &= 36k(36k^2 + 11k + 1) + 1, \end{aligned}$$

so $m - 1$ is divisible by $6k$, $12k$, and $18k$. □

***Remark* 3.10.** *[Chi09, p.415]* If it were known that there are infinitely many values of k for which all three factors of m in Proposition 3.9 are prime, then it would follow that there are infinitely many Carmichael numbers. However, while it is known by a famous theorem of Dirichlet that each factor is prime for infinitely many k, it is not known if there are infinitely many k for which all three factors are simultaneously prime. Thus it is apparently an open question whether or not there exist infinitely many Carmichael number that are products of exactly three primes.

For the rest of the subsection we will be according to [Chi09, p.415*ff*], which points out that in 1956, Erdös proposed a different way to use Korselt's criterion to produce Carmichael numbers.

Theorem 3.11. *[Chi09, p.415] Given a number L, let $\mathcal{P}$ be the set of all primes p coprime to L so that $p-1$ divides L. If C is a product of distinct primes from $\mathcal{P}$ so that $C \equiv 1 \pmod{L}$, then C is Carmichael.*

Proof. This follows quickly from Korselt's criterion. For if $C \equiv 1 \pmod{L}$, then L divides $C-1$. Each prime p dividing C is in $\mathcal{P}$, so $p-1$ divides L, hence $p-1$ divides $C-1$. □

Erdös' criterion works well if L has may divisors, so is divisible by $p-1$ for many primes p. Here is a small example.

***Example* 3.12.** *[Chi09, p.415f]* Let $L = 2^3 \cdot 3 \cdot 5 = 120$. The primes $p > 5$ so that $p-1$ divides 120 are 7, 11, 13, 31, 41, and 61. To find a Carmichael number by Erdös' criterion we must find some product C of some of these six primes so that C is congruent to 1 modulo 120.
A simple counting argument suggests that this should be possible. There are $\phi(120) = 32$ units modulo 120, and $2^6 - 1 = 63$ different products of one or more of the six primes. So we should expect perhaps two different products of the primes which are congruent to 1 modulo 120 and hence are Carmichael. Since such a product C must be congruent to 1 (mod 10), we can see easily that if 7 is a factor of C, so is 13. So we need to check all products involving three or more of the primes 11, 31, 41, and 61; and all products involving $91 = 7 \cdot 13$ and one or more of 11, 31, 41, and 61. This is a total of nineteen products. After some computation, we find that

$$\begin{aligned} 11 \cdot 31 \cdot 41 \cdot 61 &\equiv 1 \pmod{120} \\ 11 \cdot 41 \cdot 91 &\equiv 1 \pmod{120} \\ 31 \cdot 61 \cdot 91 &\equiv 1 \pmod{120} \end{aligned}$$

We have found three Carmichael numbers.

In 1992, W.R. Alford strengthened Erdös' criterion using the following idea. Pick L so that $p-1$ divides L for a large set

$$\mathcal{P} = \{p_1, p_2, \ldots, p_N\}$$

of primes. Suppose that we can find a subset, say

$$\mathcal{P}_0 = \{p_1, \ldots, p_s\}$$

where $s < N$, so that every unit modulo L can be represented by a product of distinct primes from $\mathcal{P}_0$. Then take any product q of zero or more distinct primes form remaining $N - s$ primes

$$\mathcal{P}_1 = \{p_{s+1}, \ldots, p_N\}.$$

That product q is a unit modulo L. The inverse of that unit is represented by some product q' of primes form $\mathcal{P}_0$, and $C \equiv 1 \pmod{L}$. So C is Carmichael, by Erdös' criterion.

***Example* 3.13.** *[Chi09, p.416]* Let $L = 2^6 \cdot 3^5 \cdot 5 \cdot 7 \cdot 11$. Then there are 77 primes $p > 11$ such that $p - 1$ divides L. Since $\phi(L) = 2^5 \cdot 3^4 \cdot 2 \cdot 4 \cdot 6 \cdot 10 = 1244160$, while $2^{21} = 2097152$, one would expect that if we take $\mathcal{P}_0$ to be the set of the first 21 primes that divide L, then distinct products of these primes would yield all units modulo L. If so, then the set $\mathcal{P}_1$ would contain 56 primes. Each product q of distinct primes in $\mathcal{P}_1$, when multiplied by a suitable product q' of primes in $\mathcal{P}_0$, would give a Carmichael number C. But there are 2^{56} possible products of distinct primes in $\mathcal{P}_1$. So this strategy should give us 2^{56} Carmichael numbers!

Alford did in fact better than that. He let $L = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$, and found a set $\mathcal{P}$ of 155 primes $p \geq 13$ so that $p - 1$ divides L. Now $\phi(L) = 4838400$ and $2^{27} = 134217728$. So it seems very likely, and Alford in fact showed (not by hand!), that products of the first 27 primes of $\mathcal{P}$ give all possible units modulo L. That leaves 128 primes in $\mathcal{P}$ Thus Alford found 2^{128} Carmichael numbers, one for each product of distinct primes for the last 128 primes of $\mathcal{P}$. In particular, he found a Carmichael number divisible by at least 128 primes.

3.3 Distribution and Infinitude

In the book of [Rie94, p.94f] some estimations on the number of Carmichael numbers are recapitulated. The density of pseudoprimes determines how often probable primes are composite. It is thus of interest to count the number of pseudoprimes of various types $\leq x$ and to find asymptotic formulas for their numbers as $x \to \infty$. Let $P_2(x)$ be the number of pseudoprimes $\leq x$ for base 2 and $C(x)$ the number of Carmichael numbers $\leq x$. Not too much has been proved about the behaviour of these counting functions, but some fairly precise conjectures have been made (see [Pom81]). The following inequality have been proved so far:

$$C(x) \leq x \exp\left\{-\frac{\ln x}{\ln_2 x}\left(\ln_3 x + \ln_4 x + \frac{\ln_4 x - 1}{\ln_3 x} + O\left(\left(\frac{\ln_4 x}{\ln_3 x}\right)^2\right)\right)\right\} \tag{3.2}$$

as $x \to \infty$. Here $\ln_2 x$ stands for $\ln\ln x$ and so on. Comparing these expressions with $\pi(x) \sim x/\ln x$, we can confirm our earlier assertion that the pseudoprimes for base 2 and the Carmichael numbers are scarce. To give just a few examples: for $x = 10^{20}$, $P_2(x)/\pi(x) \leq 1.43 \cdot 10^{-2}$ and $C(x)/\pi(x) \leq 7.2 \cdot 10^{-5}$ and for $x = 10^{20}$, these quotients are $\leq 7.2 \cdot 10^{-7}$ and $\leq 5.7 \cdot 10^{-16}$, respectively. Thus the fraction of probable primes $\leq x$ which actually are composite turns out to be very tiny indeed for large values of x. The following conjecture is stated, also in [Pom81]:

$$C(x) = x \exp\left\{-\frac{\ln x}{\ln_2 x}\left(\ln_3 x + \ln_4 x + \frac{\ln_4 x - 1}{\ln_3 x}\right)\right\} + O\left(\frac{\ln_4 x}{\ln_3 x}\right)^2, \qquad \text{as } x \to \infty. \tag{3.3}$$

However, statistics on these numbers show that for $10^{11} < x < 10^{16}$,

$$C(x) \approx x \exp\left\{-\frac{\ln x}{\ln_2 x} \cdot 1.86 \ln_3 x\right\}, \tag{3.4}$$

which indicates that some modification of the above conjecture might be needed. [CP05, p.134] is also concerned with the question if there is a "Carmichael number theorem", which like the prime number theorem would give an asymptotic formula for $C(x)$? So far there is not even a conjecture for what this formula may be. However, there is a somewhat weaker conjecture.

Conjecture 3.14. *The number $C(x)$ of Carmichael number not exceeding x satisfies*

$$C(x) = x^{1-(1+o(1))\ln\ln\ln x/\ln\ln x}$$

as $x \to \infty$.

It has been proved, see [Pom81] , that

$$C(x) < x^{1-\mathrm{lnlnln}x/\mathrm{lnln}x}$$

for all sufficiently large values of x.

Some more recent results on Carmichael numbers' infinitude are mentioned in [CP05, p.134]. Are there infinitely many Carmichael numbers? Again, unfortunately for primality testing, the answer is yes. This was shown in [AGP94b]. P. Erdös [Erd56] had given a heuristic argument in 1956 that not only are there infinitely many Carmichael numbers, but they are not as rare as one might expect. That is, if $C(x)$ denotes the number of Carmichael numbers up to the bound x, then Erdös conjectured that for each $\epsilon > 0$, there is a number $x_0(\epsilon)$ such that $C(x) > x^{1-\epsilon}$ for all $x \geq x_0(\epsilon)$. The proof of Alford, Granville, and Pomerance starts from the Erdös heuristic and adds some new ingredients.

Theorem 3.15 (Alford, Granville, Pomerance)**.** *[CP05, p.134]*
There are infinitely many Carmichael numbers. In particular, for x sufficiently large, the number $C(x)$ of Carmichael numbers not exceeding x satisfies $C(x) > x^{2/7}$.

[CP05, p.134] noted that the proof may be found in [AGP94b]. The "sufficiently large" in Theorem 3.15 has not been calculated, but probably it is the 96th Carmichael number, 8719309. From calculations in [Pin93] it seems likely that $C(x) > x^{1/3}$ for all $x \geq 1015$. Already at 1015, there are 105212 Carmichael numbers. Though Erdös has conjectured that $C(x) > x^{1-\epsilon}$ for $x \geq x_0(\epsilon)$, we know no numerical value of x with $C(x) > x^{1/2}$.

***Remark* 3.16.** *[Guy04, p.50]* Alford, Granville & Pomerance [AGP94b] have shown that there are infinitely many Carmichael numbers, in fact, for sufficiently large x, more than x^{β} of them less than x, where

$$\beta = \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) > 0.290306 > \frac{2}{7}$$

Erdös [Erd56] had conjectured that $(\mathrm{ln}C(x))/\mathrm{ln}x$ tends to 1 as x tends to infinity and he improved a result of Knödel [Knö53] to show that

$$C(x) < x\exp\{-c\mathrm{ln}x\mathrm{lnlnln}x/\mathrm{lnln}x\}.$$

Then Pomerance, Selfridge & Wagstaff [PSW80] proved this with $c = 1 - \epsilon$ and give a heuristic argument supporting the conjecture that the reverse inequality holds with $c = 2 + \epsilon$.

3.4 Carmichael numbers and RSA Codes

This subsection we follow solely [Chi09, p.426*ff*]. In [Chi09, Chapter l0.A] resp. appendix C we examined the RSA cryptosystem, which encrypts a message word a by replacing a by $a^e \pmod m$ where the modulus m is the product of two large prime numbers p and q. To find a large prime p we could proceed as follows: first pick an interval of numbers of the desired size and sieve out all the composite numbers with small prime numbers as factors, as in [Chi09, Section 6.G]. Then we use the $a-$pseudoprime test or the strong $a-$pseudoprime test to test the remaining unsieved numbers for primeness, as in [Chi09, Section 10.B].
Suppose, after sieving, we found a potential prime number q, and we used the $a-$pseudoprime test repeatedly, checking $a^{q-1} \equiv 1 \pmod q$ for a collection of numbers a.
If q is prime, q will pass this test for any a.
If q is composite and Carmichael, q will also pass this test for any a not relatively prime to q.
If q is composite and not Carmichael, then the set of $a \pmod q$ for which $a^{q-1} \equiv 1 \pmod q$ is a proper subgroup of the group of units of $\mathbb{Z}/q\mathbb{Z}$, so the probability that q passes the $a-$pseudoprime test for a randomly selected number a is at most $1/2$. For such numbers q, repeated testing with randomly chosen numbers a will almost surely reveal that q is composite.
Carmichael numbers are very much rarer than primes. So if we had a number q which passed repeated $a-$pseudoprime tests, it would be reasonable for us to assume that q is prime, not Carmichael.
But suppose we were wrong? Suppose q were Carmichael?
Suppose p and q are coprime Carmichael numbers. Let $m = pq$ and set up an RSA code with modulus m. Believing that p and q are primes, we would assume that $\phi(m) = (p-1)(q-1)$. As in [Chi09, Section 10.A], we would pick an encoding exponent e by choosing any number e coprime to $(p-1)(q-1)$. We would find the decoding exponent via Bezout's identity: since $(e, (p-1)(q-1)) = 1$, there is some d, k so that $ed - k(p-1)(q-1) = 1$. Then for any integer a,

$$a^{ed} = a^{1+k(p-1)(q-1)}.$$

If p, q are primes, we know by Euler's Theorem that

$$a^{1+k(p-1)(q-1)} \equiv a \pmod m.$$

But what happens if p and q are not primes, but are Carmichael numbers? Then the construction still works:

Proposition 3.17. *[Chi09, p.427] If p and q are primes or Carmichael numbers, then for any $a < m$, $a^{1+k(p-1)(q-1)} \equiv a \pmod{m}$.*

Proof. First note that since p and q are each assumed to be either prime or Carmichael, each is square-free. Since p and q are coprime, it follows that m is square-free. Hence

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{m}$$

iff

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{c}$$

where c is any prime divisor of m. If c is a prime divisor of m, then c divides p or c divides q. Suppose c divides p. If $c = p$, then $c - 1 = p - 1$; if p is Carmichael, $c - 1$ divides $p - 1$ by Korselt's criterion. Now by Fermat's theorem, for any a coprime to c,

$$a^{c-1} \equiv 1 \pmod{c},$$

so

$$a^{h(c-1)+1} \equiv a \pmod{c}$$

for every h, and in particular if $h = k(q-1)(p-1)/(c-1)$, an integer since $c - 1$ divides $p - 1$. But this last congruence is also true if a is divisible by c, and so it is true for every a. Thus for any prime c dividing m,

$$a^{(p-1)(q-1)+1} \equiv a \pmod{c}.$$

Since m is square-free, it follows that

$$a^{(p-1)(q-1)+1} \equiv a \pmod{m}.$$

for ever $a < m$, as we wished to show. □

Thus for setting up RSA codes, Carmichael numbers work as well as primes. Of course, if $m = pq$ is a product of Carmichael numbers then the prime factors of m will be much smaller than m, so will be easier to find than if p and q were prime. So the security of the RSA code will be less than it would be if p and q are primes.

4 Euler Pseudoprimes

In [Rie94, p.90f] it is annotated that due to the existence of Carmichael numbers, it is essential to improve the Fermat test. Many Carmichael numbers are revealed as composites by Euler's criterion A.4.9, so that it distinguishes primes from composites more efficiently than does Fermat's theorem. The above remark applies also to many composite numbers which are not Carmichael numbers, but which are still not shown to be composite by Fermat's theorem for a specific base a. We find for instance that

$$2^{170} \equiv 1 \pmod{341}, \quad 5^{280} \equiv 67 \pmod{561}, \quad 11^{864} \equiv 1 \pmod{1729}.$$

Since $67 \not\equiv \pm 1 \pmod{561}$, there is no need to compute Jacobi's symbol in this case. In the remaining two cases we obtain $\left(\frac{2}{341}\right) = -1$, and $\left(\frac{11}{1729}\right) = -1$, so that all these integers will be revealed as composite by Euler's criterion. Of these three numbers, 561 and 1729 are Carmichael numbers, while 341, having $2^{340} \equiv 1 \pmod{341}$, is not. According to Euler's criterion for quadratic residues, we have

$$a^{(N-1)/2} \equiv \pm 1 \pmod{N} \qquad \text{for } \gcd(a, N) = 1, \tag{4.1}$$

if N is an odd prime. Hence, (4.1) can be used as a test of compositeness on N as well as Fermat's theorem:

Theorem 4.1. *(**Euler's criterion used as compositeness test**) [Rie94, p.90] If N is odd,* $\gcd(a, N) = 1$, *and*

$$a^{(N-1)/2} \not\equiv \pm 1 \pmod{N},$$

then N is composite. If $a^{(N-1)/2} \equiv \pm 1 \pmod{N}$, then this value should be compared with the value of Jacobi's symbol $\left(\frac{a}{N}\right)$, and if

$$a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \pmod{N},$$

then N is composite. - If, however

$$a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}, \tag{4.2}$$

then the test is not conclusive.

It is further noted in [Rie94, p.90] that as in Fermat's compositeness test there are "false primes" . So there are odd composites which for certain bases a satisfy (4.2).

"This leads to the notion of an Euler pseudoprime in base a (epsp(a)), proposed by Shanks in 1962 [Sha78]" [Rib04, p.95].

4.1 Definition

Definition 4.2. *[KLS01, p.137]* The composite odd integer N is an *Euler pseudoprime to the base a* (also denoted as epsp(a)) if $\gcd(a, N) = 1$ and

$$\left(\frac{a}{N}\right) \equiv a^{(N-1)/2} \pmod{N}, \tag{4.3}$$

where $a \geq 1$ and $(\frac{a}{N})$ denotes the Jacobi symbol. Euler pseudoprimes to the base 2 will simply be called *Euler pseudoprimes*.

4.2 Properties

According to [FR07, p.222] the following observation can be made. Since $(\frac{a}{n}) = \pm 1$ it follows easily that an Euler pseudoprime to the base a must also be a pseudoprime to the base a. However, the converse is not true: there exist pseudoprimes to a base a that are not Euler pseudoprimes to that base.

***Example* 4.3.** *[Chi09, p.455]* The Carmichael number 1729 is an 11-pseudoprime but not an Euler 11-pseudoprime. To see the latter, we have

$$\left(\frac{11}{1729}\right) = \left(\frac{1729}{11}\right) = \left(\frac{2}{11}\right) = -1$$

since $11 \equiv 3 \pmod 8$; on the other hand, observing that $1729 = 7 \cdot 13 \cdot 19$ we have

$$\begin{aligned} 11^{864} &\equiv (11^6)^{144} \equiv 1 \pmod 7 \\ 11^{864} &\equiv (11^{12})^{72} \equiv 1 \pmod{13} \\ 11^{864} &\equiv (11^{18})^{48} \equiv 1 \pmod{19} \end{aligned}$$

by Fermat's Theorem. Thus $11^{864} \equiv 1 \pmod{1729}$.

"What is crucial in describing this kind of primality test is that there are no "Carmichael-type" numbers for Euler pseudoprimes" [FR07, p.222]. It is written in [Rib04, p.96] that in 1976, Lehmer [Leh76] showed that if n is odd composite, then it cannot be an epsp(a), for every a, $1 < a < n$, $\gcd(a, n) = 1$. [KLS01, p.137] mentions that it is proved in [SS77] that a composite odd integer N can be an Euler pseudoprime for at most $\frac{1}{2}\phi(n)$ bases a, $1 \leq a < n$, $\gcd(a, n) = 1$. Thus, if the base a is chosen randomly, the probability that a composite integer N is an Euler pseudoprime to the base a is less than or equal to $\frac{1}{2}$.

Theorem 4.4 (**Solovay, Strassen**). *[FR07, p.222ff] If n is an odd composite integer, then n is an Euler pseudoprime for at most one-half of the bases b with $1 < b < n$ and $\gcd(b, n) = 1$.*

Proof. Suppose that n is odd and composite. We first show that in this case if n is not an Euler pseudoprime for at least one base b then it is not an Euler pseudoprime for at least half of the bases b with $1 < b < n$, $\gcd(b, n) = 1$. We then show that if n is odd and composite there is a base b for which n is not an Euler pseudoprime.
Suppose that n is odd and composite and suppose that n is not an Euler pseudoprime to the base b. That is,

$$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$

If n is not an Euler pseudoprime to any base then certainly it is not an Euler pseudoprime for at least half of the possible bases. Suppose then that n is an Euler pseudoprime to the base b_1, so that

$$b_1^{\frac{n-1}{2}} \equiv \left(\frac{b_1}{n}\right) \pmod{n}. \tag{4.4}$$

Then

$$(bb_1)^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} b_1^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \left(\frac{b_1}{n}\right) \not\equiv \left(\frac{b}{n}\right)\left(\frac{b_1}{n}\right) = \left(\frac{bb_1}{n}\right) \pmod{m}. \tag{4.5}$$

Hence n is not an Euler pseudoprime to the base bb_1. Therefore for every base b_i for which n is an Euler pseudoprime, n is not an Euler pseudoprime for the base bb_i.
Further, if b_i, b_j are distinct (mod n) bases for which n is an Euler pseudoprime, then bb_i is not congruent to bb_j mod n. It follows that if $\{b_1, \ldots, b_k\}$ are the distinct bases for which n is an Euler pseudoprime then $\{bb_i, \ldots, bb_k\}$ are distinct bases for which n is not an Euler pseudoprime. Therefore there are at least as many bases for which n is not an Euler pseudoprime as there are bases for which it is. We conclude then that if there exists at least one base b for which n is not an Euler pseudoprime then n is an Euler pseudoprime for at most one-half of the possible bases. We now show that there must exist a base b for which n is not an Euler pseudoprime. Suppose first that n is not square-free, so that there exists a prime p with $p^2|n$. Let g be a generator of the multiplicative group of $\mathbb{Z}_{p^2}$. Then as in the proof of the Korselt criterion, g has exact multiplicative order $\phi(p^2) = p(p-1)$. Let b solve the pair of congruences

$$b \equiv g \pmod{p^2},$$
$$b \equiv 1 \pmod{\frac{n}{p^2}}.$$

Then suppose that $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. It follows that $p(p-1)|\frac{(n-1)}{2}$, which is impossible since $p^2|n$. Next suppose that $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Then $b^{n-1} \equiv 1 \pmod{n}$, so $b^{n-1} \equiv 1 \pmod{p^2}$. It follows that $p(p-1)|n-1$. But then again $p|n-1$ a contradiction. Hence if n is not square-free, then b as chosen above is a base for which n is not an

Euler pseudoprime. Now suppose that n is square-free with $n = p_1 \cdots p_k$ with p_i distinct primes. Let g be a non-square mod p_1. Recall that there are only $\frac{p_1-1}{2}$ squares mod p_1, so such non-squares exist. Hence $(\frac{g}{p_1}) = -1$. Choose a base b satisfying the simultaneous congruences

$$\begin{aligned} b &\equiv g \pmod{p_1}, \\ b &\equiv 1 \pmod{p_i}, \quad i = 2, \ldots, k, \end{aligned}$$

which exists by the Chinese remainder theorem. We then have for the Jacobi symbol

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_k}\right)$$

but $(\frac{b}{p_1}) = -1$ since $b \equiv g \pmod{p_1}$ and $(\frac{b}{p_i}) = (\frac{1}{p_i}) = 1$. Hence

$$\left(\frac{b}{n}\right) = -1$$

If n were an Euler pseudoprime to the base b then

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n},$$

so that

$$b^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

But then

$$b^{\frac{n-1}{2}} \equiv -1 \pmod{p_2},$$

which is a contradiction since $b \equiv 1 \pmod{p_2}$. Therefore n cannot be an Euler pseudoprime to the base b. Hence in each case there does exist a base for which n is not an Euler pseudoprime, proving the theorem. □

[FR07, p.224] emphasises the following. This Theorem is the basis for the Solovay-Strassen primality test. Suppose that we are given an odd integer n. Choose k integers $b_1, b_2, \ldots, b_k$ at random with $1 < b_i < n$. If for some i we have $\gcd(b_i, n) > 1$ then n is composite. If all b_i are relatively prime to n, then for each b_i compute

(1) $b_i^{\frac{n-1}{2}} \bmod n$ and

(2) $(\frac{b_i}{n}) \bmod n$.

If (1) does not equal (2) for some b_i then n is composite. Finally, if

$$b_i^{\frac{n-1}{2}} \equiv \left(\frac{b_i}{n}\right) \pmod{n} \tag{4.6}$$

for all $i = 1, \ldots, k$ then the probability that n is not prime is less than $(\frac{1}{2})^k$. To see this notice that if n passes the conditions for b_1 then the probability of being composite from the Solovay-Strassen result is less than $\frac{1}{2}$. But b_2 is chosen randomly, so the events that n passes the conditions for b_1 and b_2 are independent. Hence the probability that n passes the conditions for both b_1 and b_2 is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$, and so on.

Algorithm 4.5. Solovay-Strassen test Input an odd integer n

1: Choose k random integers $b_1, \ldots, b_k$ with $1 < b_i < n$

2: For $i = 1, \ldots, k$

   a: Compute $\gcd(b_i, n)$ (by the Euclidean algorithm)
      i: If $\gcd(b_i, n) > 1$, then n is composite and stop

   b: Compute (1) $b_i^{\frac{n-1}{2}} \bmod n$ and (2) $(\frac{b_i}{n}) \bmod n$
      i: If (1) $\neq$ (2), then n is composite and stop

3: The probability that n is prime is greater then $1 - \frac{1}{2^k}$

4.3 Distribution and Infinitude

According to [Rib04, p.96] in 1986, Kiss, Phong & Lieuwens [KPL86] showed that given $a \geq 2$, $k \geq 2$, and $d \geq 2$, there exist infinitely many epsp(a), which are the product of k distinct primes and are congruent to 1 modulo d. Analogously to $B_{psp}(n)$ on page 16 we can find the following for Euler pseudoprimes:
Let n be an odd composite integer. Denote by $B_{\text{epsp}}(n)$ the number of bases a, $1 < a < n$, $\gcd(a, n) = 1$, such that n is an epsp(a). Monier showed in 1980 [Mon80] that

$$B_{\text{epsp}}(n) = \delta(n) \prod_{p|n} \gcd\left(\frac{n-1}{2}, p-1\right) - 1.$$

Here

$$\delta(n) = \begin{cases} 2 & \text{if } v_2(n) - 1 = \min_{p|n}\{v_2(p-1)\}; \\ \frac{1}{2} & \text{if there exist a prime } p \text{ dividing } n \text{ such that} \\ & v_p(n) \text{ is odd and } v_2(p-1) < v_2(n-1), \\ 1 & \text{otherwise,} \end{cases}$$

and for any integer m and prime p, $v_p(m)$ denotes the exponent of p in the factorization of m, that is, the $p-$adic value of m.

5 Strong Pseudoprimes

[CP05, p.135] gives the following motivation for introducing a new type of primality test. The concept of Fermat pseudoprimes, developed in the previous section, is a good one, since it is easy to check and for each base $a > 1$ there are few pseudoprimes compared with primes (Theorem 2.7). However, there are composites, the Carmichael numbers, for which (A.11) is useless as a means of recognizing them as composite. As we have seen, there are infinitely many Carmichael numbers. There are also infinitely many Carmichael numbers that have no small prime factor (see [AGP94b]), so that for these numbers, even the slightly stronger test (A.12) is computationally poor. We would ideally like an easy test for which there are no pseudoprimes. Failing this, we would like a family of tests, such that each composite is not a pseudoprime for a fixed, positive fraction of the tests in the family. The Fermat family does not meet this goal, since there are infinitely many Carmichael numbers. However, a slightly different version of Fermat's little theorem does meet this goal.

Theorem 5.1. *[CP05, p.135] Suppose that n is an odd prime and $n - 1 = 2^s t$, where t is odd. If a is not divisible by n then*

$$\begin{aligned} &\textit{either} \quad a^t \equiv 1 \pmod{n} \\ &\quad \textit{or} \quad a^{2^i t} \equiv -1 \pmod{n} \quad \textit{for some } i \textit{ with } 0 \leq i \leq s-1. \end{aligned} \tag{5.1}$$

[CP05, p.135] states that the proof of Theorem 5.1 uses only Fermat's little theorem in the form (A.12) and the fact that for n an odd prime, the only solutions to $x^2 \equiv 1 \pmod{n}$ in $\mathbb{Z}_n$ are $x \equiv \pm 1 \pmod{n}$. We leave the details to the reader. In analogy to probable primes, we can now define a strong probable prime base a. This is an odd integer $n > 3$ for which (5.1) holds for a, where $1 < a < n - 1$. Since every strong probable prime base a is automatically a probable prime base a, and since every prime greater than $a+1$ is a strong probable prime base a, the only difference between the two concepts is that possibly fewer composites pass the strong probable prime test.

The Strong a-Pseudoprime Test. *[Chi09, p.419]*
Suppose m is an odd number we wish to test for primeness. Write $m - 1 = 2^e q$ where q is odd and $e > 0$. Suppose a is a number coprime to m such that either $a^q \equiv 1 \pmod{m}$ or there is some $k < e$ so that $a^{2^k q} \equiv -1 \pmod{m}$. Then m passes the strong a-pseudoprime test. The test is called the strong a-pseudoprime test because a number that passes the strong $a-$pseudoprime tests will certainly pass the a-pseudoprime test. For if either $a^q \equiv 1 \pmod{m}$ or $a^{2^k q} \equiv -1 \pmod{m}$ for some $k < e$, then $a^{2^e q} \equiv 1 \pmod{m}$. We will see shortly that any prime number m passes the strong a-pseudoprime test for all a, $1 \leq a < m$.

Or in an even more structured way:

Algorithm 5.2. Strong probable prime test *[CP05, p.135f]*
We are given an odd number $n > 3$, represented as $n = 1 + 2^s t$, with t odd. We are also given an integer a with $1 < a < n-1$. This algorithm returns either "n is a strong probable prime base a" or "n is composite".

1. (Odd part of $n-1$)
   $b = a^t \bmod n$; // Use recursive power algorithm [CP05, p.86]
   if($b == 1$ or $b == n-1$) return "n is a strong probable prime base a";

2. (Power of 2 in $n-1$)
   for($j \in [1, s-1]$) { // j is a dummy counter.
   $b = b^2 \bmod n$;
   if($b == n-1$) return "n is a strong probable prime base a";
   }
   return "n is composite";

As mentioned in [CP05, p.136] this test was first suggested in [Art67], and a decade later, J. Selfridge rediscovered the test and popularized it.
We now consider the possibility of showing that an odd number n is composite by showing that (5.1) fails for a particular number a. For example, we saw in the previous section that 341 is pseudoprime base 2. But (5.1) does not hold for $n = 341$ and $a = 2$. Indeed, we have $340 = 2^2 \cdot 85$, $2^{85} \equiv 32 \pmod{341}$, and $2^{170} \equiv 1 \pmod{341}$. In fact, we see that 32 is a non-trivial square root of 1 (mod 341). Now consider the pair $n = 91$ and $a = 10$. We have $90 = 2^1 \cdot 45$ and $10^{45} \equiv -1 \pmod{91}$. So (5.1) holds. Thus, 341 is not a strong pseudoprime base 2, while 91 is a strong pseudoprime base 10. J. Selfridge proposed using Theorem 5.1 as a pseudoprime test in the early 1970s, and it was he who coined the term "strong pseudoprime".

5.1 Definition

Definition 5.3. *[Chi09, p.419]* A composite number m that passes the strong $a-$pseudoprime test is called a *strong $a-$pseudoprime*.

or more precisely:

Definition 5.4. *[CP05, p.136]* We say that n is a *strong pseudoprime base a* (also denoted as spsp(a)) if n is an odd composite, $n - 1 = 2^s t$, with t odd and (5.1) holds.

[Chi09, p.419] shows another way of looking at the strong $a-$pseudoprime test. Let $m - 1 = 2^e q$, with q odd, and consider the set of numbers mod m,

$$\left(a^q, a^{2q}, \ldots, a^{2^e q}\right),$$

that we obtain, starting from a^q modulo m, by successively squaring modulo m. We will call this sequence of numbers the "strong a-pseudoprime sequence" .
Suppose $a^{2^e q} \equiv 1 \pmod{m}$, so that m passes the $a-$pseudoprime test. Suppose also that either:
all numbers in the sequence are $1 \pmod{m}$ or
the rightmost number not $\equiv 1 \pmod{m}$ is $\equiv -1 \pmod{m}$. Then m passes the strong $a-$pseudoprime test. The strong $a-$pseudoprime sequence in that case looks like

$$(1, 1, \ldots, 1) \quad \text{or} \quad (\ldots, -1, 1, \ldots, 1).$$

On the other hand, it m is an $a-$pseudoprime but the strong $a-$pseudoprime sequence for m looks like

$$(\ldots, b, 1, \ldots, 1).$$

with $b \not\equiv 1$ or $-1 \pmod{m}$, then m fails the strong $a-$pseudoprime test, so m must be composite. The number m cannot be prime because b is a square root of 1 modulo m, and so 1 has at least three square roots $1, -1, b \pmod{m}$ (see Proposition 5.5 below.)

Proposition 5.5. *[Chi09, p.420] If m fails the strong $a-$pseudoprime test for some a not divisible by m, then m is composite. If m is an $a-$pseudoprime but not a strong $a-$pseudoprime, the a yields a factorization of m.*

Proof. Write $m - 1 = 2^e q$, where q is odd. If $a^{2^e q} \not\equiv 1 \pmod{m}$ then m is composite by Fermat's theorem. Suppose $a^{2^e q} \equiv 1 \pmod{m}$ and suppose the sequence

$$(a^q, a^{2q}, \ldots, a^{2^e q})$$

is congruent modulo m to

$$(\ldots, b, 1, \ldots, 1)$$

where $b \equiv a^{2^k q} \pmod{m}$ is the rightmost element of the sequence that is not congruent to $1 \pmod{m}$. If m fails the strong $a-$pseudoprime test, $b \not\equiv 1$ or $-1 \pmod{m}$. Now b^2 is congruent modulo m to the element of the sequence immediately to the right of b, so $b^2 \equiv 1 \pmod{m}$. Hence m divides $b^2 - 1 = (b-1)(b+1)$. Since $b \not\equiv 1$ or $-1 \pmod{m}$, m does not divide $b - 1$ or $b + 1$. So m cannot be prime, and, in fact, $m = (m, b-1)(m, b+1)$ is a non-trivial factorization of m. □

***Example* 5.6.** *[Chi09, p.420]* Let $m = 91$. We ignore the fact 91 is easily factored. Since $m - 1 = 90 = 2 \cdot 45$, the strong $a-$pseudoprime sequence is short: (a^{45}, a^{90}). We try $a = 3$. Then $3^{45} \equiv 27$ while $3^{90} \equiv 1 \pmod{91}$. So while 91 is a 3-pseudoprime, the strong 3-pseudoprime sequence is (27, 1), so 91 fails the strong 3-pseudoprime test, and 91 is not prime. (In particular, 27,1, and -1 are three square roots of 1 modulo

91). If we try $a = 2$, then $2^{90} \equiv 64 \pmod{91}$: the strong 2-pseudoprime sequence is (57,64). So 91 is not a 2-pseudoprime, hence is not a strong 2-pseudoprime.

***Example* 5.7.** *[Chi09, p.420]* Let $m = 97$, a prime. then $m - 1 = 96 = 2^5 \cdot 3$, so modulo 97, the strong $a-$pseudoprime sequence is

$$(a^3, a^6, a^{12}, a^{24}, a^{48}, a^{96}).$$

Once we find $a^3 \pmod{97}$, the rest of the sequence is determined by squaring modulo 97, so the sequence is easy to compute for any a. Here is a table of some examples:

For $a =$	the sequence is
2	$(8, 64, 22, -1, 1, 1)$
3	$(27, 50, -22, -1, 1, 1)$
5	$(28, 8, 64, 22, -1, 1)$
13	$(63, 89, 64, 22, -1, 1, 1)$
17	$(63, 89, 64, 22, -1, 1)$
61	$(1, 1, 1, 1, 1, 1)$

Thus 97 passes the strong $a-$pseudoprime test for all of these a's.

5.2 Properties

Pursuant to [KLS01, p.137] it is evident that strong pseudoprimes to the base a are (Fermat) pseudoprimes to the base a. Note that

$$a^{N-1} - 1 = a^{2^s t} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1) \cdots (a^{2^{s-1}t} + 1). \tag{5.2}$$

If N is prime, then by Fermat's little theorem

$$a^{N-1} - 1 \equiv 0 \pmod{N},$$

which implies that one of the factors on the right-hand side of (5.2) is congruent to 0 (mod N); hence, N satisfies (5.1). [CP05, p.136] indicates that the example with $n = 341$ and $a = 2$ shows that the converse is false.

Moreover it is written in [Rib04, p.97] that Selfridge showed (see the proof in Williams' paper, 1978, [Wil78]) that every spsp(a) is an epsp(a). There are partial converses. By Malm (1977) [Mal77]: if $n \equiv 3 \pmod{4}$ and n is an epsp(a), then n is a spsp(a).

By Pomerance, Selfridge & Wagstaff (1980) [PSW80]: if n is odd, $(a|n) = -1$ and n is an epsp(a), then n is also a spsp(a). In particular, if $n \equiv 5 \pmod{8}$ and n is an epsp(2), then it is a spsp(2).

Theorem 5.8. *[KLS01, p.138] If N is a strong pseudoprime to the base a, then N is an Euler pseudoprime to the base a. Moreover, if $N \equiv 3 \pmod 4$ and N is an Euler pseudoprime to the base a, then N is a strong pseudoprime to the base a.*

Proof. The proof of the first assertion is due to Selfridge (see [Wil78, Section 17]). The second assertion was proved in [Mal77]. □

Continuing with [KLS01, p.138], in Theorem 1.8 and 1.7 it was proved that both F_m and M_p are pseudoprimes if they are composite. Theorem 5.9 below shows, in addition, that composite Fermat numbers and composite Mersenne numbers are also Euler pseudoprimes and strong pseudoprimes.

Theorem 5.9. *[KLS01, p.138f] Let F_m be a composite Fermat number and let $M_p = 2^p - 1$ be a composite Mersenne number, where p is a prime. Then F_m and M_p both are Euler pseudoprimes and strong pseudoprimes.*

Proof. We note that $m \geq 5$ and $p \geq 11$. We will show that F_m and M_p are both Euler pseudoprimes and strong pseudoprimes without resort to Theorem 5.8. Note that $\left(\frac{2}{F_m}\right) = 1$ and $\left(\frac{2}{M_p}\right) = 1$ by property (vii) of Theorem 2.3. in [KLS01, p.25].
We first treat the Fermat number F_m. It is clear that

$$2^{2^m} \equiv -1 \pmod{F_m}, \tag{5.3}$$

and hence F_m is a strong pseudoprime. Furthermore, for $m \geq 5$,

$$(F_m - 1)/2 = 2^{2^m - 1} > 2^m.$$

Let $k \geq 1$ be such that

$$\frac{(F_m - 1)/2}{2^m} = 2^k.$$

Then by (5.3),

$$2^{(F_m-1)/2} = \left(2^{2^m}\right)^{2^k} \equiv (-1)^{2^k} \equiv 1 \equiv \left(\frac{2}{F_m}\right) \pmod{F_m},$$

and thus F_m is an Euler pseudoprime.
We now consider the Mersenne number M_p. Note that $(M_p - 1)/2 = 2^{p-1} - 1$ is an odd integer. By (1.5) in the proof of Theorem 1.7,

$$2^{(M_p-1)/2} \equiv 1 \equiv \left(\frac{2}{M_p}\right) \pmod{M_p}.$$

Hence, M_p is both a strong pseudoprime and an Euler pseudoprime. □

Theorem 5.10. *[KLS01, p.139] If N is a pseudoprime, then $2^N - 1$ is a strong pseudoprime.*

Proof. Notice that $(2^N - 2)/2 = 2^{N-1} - 1$ is an odd integer. By (1.3) in the proof of Theorem 1.4,

$$2^{(2^N-2)/2} \equiv 1 \pmod{2^N - 1},$$

and hence $2^N - 1$ is a strong pseudoprime. □

Another property of strong pseudoprimes is noted in [Rib04, p.97]. Similarly to the case of Fermat pseudoprimes there exist strong pseudoprimes with arbitrarily large numbers of distinct prime factors. But the most important property of strong pseudoprimes - especially for primality testing - is, that there are no odd composite numbers, which can be strong pseudoprimes for every possible base a.

[Chi09, p.422] discusses this issue as follows: Let $U = U_m$ be the set of units of $\mathbb{Z}/m\mathbb{Z}$, and let $\phi(m)$ be the number of elements of U (for used results see [Chi09, Section 11.A and 19.E]).
Now we show that there are no "strong" Carmichael numbers. In other words, every odd composite number m fails the strong $a-$pseudoprime test for some number a coprime to m.
First, some alternate terminology.

Definition 5.11. *[Chi09, p.422]* If for some number a, the number m fails the strong $a-$pseudoprime test, then m is necessarily a composite number: in that case the number a is called a **witness** to the compositeness of m, or, for short, a witness for m. If m is composite but is a strong $a-$pseudoprime, the number a is called a false witness for m.

***Remark* 5.12.** *[Chi09, p.422]* M. O. Rabin [Rab80] proved a stronger version of Theorem 5.13. He showed that for m odd and composite, at most one fourth of the numbers $a < m$ are false witnesses. His result leads to the Miller-Rabin test, which will discussed later in this section. Before beginning the proof of Theorem 5.13, we recall from [Chi09, Chapter 11] the subgroups of roots of unity of the multiplicative group $U = U_m$ of units of $\mathbb{Z}/m\mathbb{Z}$. Let

$$U(k) = \left\{[a] \text{ in } U | [a]^k = [1]\right\},$$

the group of k-roots of unity in U, for any number k. Then $U(k)$ is a subgroup of U. A number m is Carmichael if and only if $a^{m-1} \equiv 1 \pmod{m}$ for all a coprime to m, hence if and only if $U(m-1) = U$.

Theorem 5.13. *[Chi09, p.422f] If m is an odd composite number, then at most half of the numbers $a < m$ are false witnesses for m.*

Proof. We consider three cases:
Case 1: If a number m is not a Carmichael number, then $U(m-1)$, the set of $[a]$ in U for which m is an $a-$pseudoprime, is a proper subgroup of U. As showed in [Chi09,

Section 11.D], if $q \geq 2$ is the number of cosets of $U(m-1)$ in U, that is, the index of $U(m-1)$ in U, then at most $1/q$ of the units in U are not witnesses for m.
Write $m-1 = 2^e t$ for odd t, and assume that m is Carmichael. Then $U = U(m-1) = U(2^e t)$. Let s be the least number so that $U = U(2^s t)$. Then $s > 0$ since $[-1]^t = [-1]$ is not in $U(2^0 t)$. Then

$$U(2^{s-1}t) = \{[a] \in U | [a]^{2^{s-1}t} = 1\}$$

is a proper subgroup of U. So the index of $U(2^{s-1}t)$ in U is $q \geq 2$.
Case 2: Suppose there is no $[b]$ so that $[b]^{2^{s-1}t} = [-1]$. Then every $[a]$ not in $U(2^{s-1}t)$ is a witness to the compositeness of m, and so at most $1/q$ of the units in U are false witnesses for m.
Case 3: Suppose $[b]$ in U satisfies $[b]^{2^{s-1}t} = [-1]$. Then every element $[b']$ of $[b]U(2^{s-1}t)$ satisfies $[b']^{2^{s-1}t} = [-1]$. Moreover, if $[b']^{2^{s-1}t} = [-1]$, then $[a] = [b'][b]^{-1}$ in $U(2^{s-1}t)$. Hence every false witness for m is in $U(2^{s-1}t)$ or in $[b]U(2^{s-1}t)$. We construct two other cosets of $U(2^{s-1}t)$. Since m is Carmichael, m is divisible by at least two odd primes. So write $m = fg$ with f, g coprime. Since $b^{2^{s-1}t} \equiv -1 \pmod{m}$, we have $b^{2^{s-1}t} \equiv -1 \pmod{f}$ and also $\pmod{g}$. Let c satisfy $c \equiv b \pmod{f}$, $c \equiv 1 \pmod{g}$, and let d satisfy $d \equiv 1 \pmod{f}$, $d \equiv b \pmod{g}$. Then

$$c^{2^{s-1}t} \equiv -1 \pmod{f}, \quad c^{2^{s-1}t} \equiv 1 \pmod{g},$$

while

$$d^{2^{s-1}t} \equiv 1 \pmod{f}, \quad d^{2^{s-1}t} \equiv -1 \pmod{g}.$$

Thus $1, b^{2^{s-1}t}, c^{2^{s-1}t}$, and $d^{2^{s-1}t}$ are different square roots of 1 in U, and so

$$U(2^{s-1}t), [b]U(2^{s-1}t), [c]U(2^{s-1}t), [d]U(2^{s-1}t)$$

are distinct cosets. All the false witnesses for m lie in the first two of these cosets. Thus there are at least as many witnesses for m as there are false witnesses. □

For examples see [Chi09, p.423]

Following [CP05, p.136*ff*] the original result mentioned above will be proven. For an odd composite integer n we shall let

$$\mathcal{S}(n) = \{a \pmod{n} : n \text{ is a strong pseudoprime base } a\} \tag{5.4}$$

and let $S(n) = \#\mathcal{S}(n)$. The following theorem was proved independently in [Mon80] and [Rab80].

Theorem 5.14. *[CP05, p.136] For each odd composite integer $n > 9$ we have $S(n) \leq \frac{1}{4}\varphi(n)$.*

***Remark* 5.15.** *[CP05, p.136]* Recall that $\varphi(n)$ is Euler's function evaluated at n. It is the number of integers in $[1, n]$ coprime to n; that is, the order of the group $\mathbb{Z}_n^*$. If we know the prime factorization of n, it is easy to compute $\varphi(n)$: We have $\varphi(n) = n\prod_{p|n}(1 - 1/p)$, where p runs over the prime factors of n.

Before proving Theorem 5.14 [CP05, p.138] first establishes some lemmas.

Lemma 5.16. *[CP05, p.139] Say n is an odd composite with $n - 1 = 2^s t$, t odd. Let $\nu(n)$ denote the largest integer such that $2^{\nu(n)}$ divides $p - 1$ for each prime p dividing n. If n is a strong pseudoprime base a, then $a^{2^{\nu(n)-1}t} \equiv \pm 1 \pmod n$.*

Proof. If $a^t \equiv 1 \pmod n$, it is clear that the conclusion of the lemma holds. Suppose we have $a^{2^i t} \equiv -1 \pmod n$ and let p be a prime factor of n. Then $a^{2^i t} \equiv -1 \pmod p$. If k is the order of $a \pmod p$ (that is, k is the least positive integer with $a^k \equiv 1 \pmod p$), then k divides $2^{i+1}t$, but k does not divide $2^i t$. Thus the exact power of 2 in the prime factorization of k must be 2^{i+1}. But also k divides $p - 1$, so that $2^{i+1}|p - 1$. Since this holds for each prime p dividing n, we have $i + 1 \leq \nu(n)$. Thus, $a^{2^{\nu(n)-1}t} \equiv 1 \pmod n$ or $-1 \pmod n$ depending on whether $i + 1 < \nu(n)$ or $i + 1 = \nu(n)$. □

For the next lemma, let

$$\bar{\mathcal{S}}(n) = \left\{a \pmod n : a^{2^{\nu(n)-1}t} \equiv \pm 1 \pmod n\right\}, \quad \bar{S}(n) = \#\bar{\mathcal{S}}(n). \tag{5.5}$$

Lemma 5.17. *[CP05, p.139] Recall the notation in Lemma 5.16 and (5.5). Let $\omega(n)$ be the number of different prime factors of n. We have*

$$\bar{S}(n) = 2 \cdot 2^{(\nu(n)-1)\omega(n)} \prod_{p|n} \gcd(t, p - 1).$$

Proof. Let $m = 2^{\nu(n)-1}t$. Suppose that the prime factorization of n is $p_1^{j_1}p_2^{j_2}\cdots p_k^{j_k}$, where $k = \omega(n)$. We have that $a^m \equiv 1 \pmod n$ if and only if $a^m \equiv 1 \pmod{p_i^{j_i}}$ for $i = 1, 2, \ldots, k$. For an odd prime p and positive integer j, the group $\mathbb{Z}_{p^j}^*$ of reduced residues modulo p^j is cyclic of order $p^{j-1}(p-1)$; that is, there is a primitive root modulo p^j.(Compare [CP05, Theorem 2.2.5.]) Thus, the number of solutions $a \pmod{p_i^{j_i}}$ to $a^m \equiv 1 \pmod{p_i^{j_i}}$ is

$$\gcd(m, p_i^{j_i-1}(p_i - 1)) = \gcd(m, p_i - 1) = 2^{\nu(n)-1} \cdot \gcd(t, p_i - 1).$$

(Note that the first equality follows from the fact that m divides $n-1$, so is not divisible by p_i.) We conclude, via the Chinese remainder theorem, that the number of solutions

$a \pmod n$ to $a^m \equiv 1 \pmod n$ is

$$\prod_{i=1}^{k} \left(2^{\nu(n)-1} \cdot \gcd(t, p_i - 1)\right) = 2^{(\nu(n)-1)\omega(n)} \prod_{p|n} \gcd(t, p-1).$$

To complete the proof we must show that there are exactly as many solutions to the congruence $a^m \equiv -1 \pmod n$. Note that $a^m \equiv 1 \pmod{p_i^{j_i}}$ if and only if $a^{2m} \equiv 1 \pmod{p_i^{j_i}}$ and $a^m \not\equiv 1 \pmod{p_i^{j_i}}$. Since $2^{\nu(n)}$ divides $p_i - 1$ it follows as above that the number of solutions to $a^m \equiv -1 \pmod{p_i^{j_i}}$ is

$$2^{\nu(n)} \cdot \gcd(t, p_i - 1) - 2^{\nu(n)-1} \cdot \gcd(t, p_i - 1) = 2^{\nu(n)-1} \cdot \gcd(t, p_i - 1).$$

Thus there are just as many solutions to $a^m \equiv 1 \pmod n$ as there are to $a^m \equiv -1 \pmod n$, and the lemma is proved. □

Proof of Theorem 5.14. From Lemma 5.16 and (5.5), it will suffice to show that $\bar{S}(n)/\varphi(n) \leq 1/4$ whenever n is an odd composite that is grater than 9. From Lemma 5.17, we have

$$\frac{\varphi(n)}{\bar{S}(n)} = \frac{1}{2} \prod_{p^\alpha || n} p^{\alpha-1} \frac{p-1}{2^{\nu(n)-1} \gcd(t, p-1)},$$

where the notation $p^\alpha || n$ means p^α is the exact power of the prime p in the prime factorization of n. Each factor $(p-1)/(2^{\nu(n)-1} \gcd(t, p-1))$ is an even integer, so that $\varphi(n)/\bar{S}(n)$ is an integer. In addition, if $\omega(n) \geq 3$, it follows that $\varphi(n)/\bar{S}(n) \geq 4$. If $\omega(n) = 2$ and n is not square-free, the product of the various $p^{\alpha-1}$ is at least 3, so that $\varphi(n)/\bar{S}(n) \geq 6$.
Now suppose $n = pq$, where $p < q$ are primes. If $2^{\nu(n)+1} | q-1$, then $2^{\nu(n)-1} \gcd(t, q-1) \leq (q-1)/4$ and $\varphi(n)/\bar{S}(n) \geq 4$. We may suppose then that $2^{\nu(n)} || q-1$. Note that $n - 1 \equiv p - 1 \pmod{q-1}$, so that $q - 1$ does not divide $n - 1$. This implies there is an odd prime dividing $q - 1$ to a higher power than it divides $n - 1$; that is, $2^{\nu(n)-1} \gcd(t, q-1) \leq (q-1)/6$. We conclude in this case that $\varphi(n)/\bar{S}(n) \geq 6$.
Finally, suppose that $n = p^a$, where $a \geq 2$. Then $\varphi(n)/\bar{S}(n) = p^{a-1}$, so that $\varphi(n)/\bar{S}(n) \geq 5$, except when $p^a \geq 9$. □

Proceeding with [CP05, p.140*ff*] we have seen in Theorem 5.14 that an odd composite number n has at least $3n/4$ witnesses in the interval $[1, n-1]$. Let $W(n)$ denote the least of the witnesses for n. Then $W(n) \geq 2$. In fact, for almost all odd composites, we have $W(n) = 2$. This is an immediate consequence of Theorem 2.7. The following theorem shows that $W(n) \geq 3$ for infinitely many odd composite numbers n.

Theorem 5.18. *[CP05, p.140] If p is a prime larger than 5, then $n = (4^p + 1)/5$ is a strong pseudoprime base 2, so that $W(n) \geq 3$*

Proof. We first show that n is a composite integer. Since $4^p \equiv (-1)^p \equiv -1 \pmod 5$, we see that n is an integer. That n is composite follows form the identity

$$4^p + 1 = (2^p - 2^{(p+1)/2} + 1)(2^p + 2^{(p+1)/2} + 1).$$

Note that $2^{2p} \equiv -1 \pmod n$, so that if m is odd, we have $2^{2pm} \equiv -1 \pmod n$. but $n - 1 = 2^2 t$, where t is odd and a multiple of p, the latter following from Fermat's little Theorem A.5.10. Thus, $2^{2t} \equiv -1 \pmod n$, so that n is a strong pseudoprime base 2. □

[CP05, p.140f] notes that it is natural to ask whether $W(n)$ can be arbitrarily large. In fact, this question is crucial. If there is a number B that is not too large such that every odd composite number n has $W(n) \leq B$, then the whole subject of testing primality becomes trivial. One would just try each number $a \leq B$ and if (5.1) holds for each such a, then n is prime. Unfortunately, there is no such number B. The following result is shown in [AGP94a].

Theorem 5.19. *[CP05, p.141] There are infinitely many odd composite number n with*

$$W(n) > (\ln n)^{1/(3 \ln \ln \ln n)}.$$

In fact, the number of such composite numbers n up to x is at least

$$x^{1/35\,(\ln \ln \ln x)}$$

when x is sufficiently large.

Failing a universal bound B, perhaps there is a slowly growing function of n which is always greater than $W(n)$. Based on [Mil76], the following result is proved in [Bac85].

Theorem 5.20. *[CP05, p.141] On the ERH (extended Riemann Hypothesis B.2), $W(n) < 2 \ln^2 n$ for all odd composite number n.*

Proof. Let n be an odd composite. [CP05, Exercise 3.19] says that $W(n) < \ln^2 n$ if n is divisible by the square of a prime, and this result is not conditional on any unproven hypotheses. We thus may assume that n is square-free. Suppose p is a prime divisor of n with $p - 1 = 2^{s'} t'$, t' odd. Then the same considerations that were used in the proof of Lemma 5.16 imply that if (5.1) holds, then $(a/p) = -1$ if and only if $a^{2^{s'-1} t'} \equiv -1 \pmod n$. Since n is odd, composite, and square-free, it must be that n is divisible by two different odd primes, say p_1, p_2. Let $p_i - 1 = 2^{s_i} t_i$, t_i odd, for $i = 1, 2$, with $s_1 \leq s_2$. Let $\chi_1(m) = (m/p_1 p_2)$, $\chi_2(m) = (m/p_2)$, so that χ_1 is a character to the modulus $p_1 p_2$ and χ_2 is a character to the modulus p_2. First, consider the case $s_1 = s_2$. Under the assumption of the extended Riemann hypothesis, [CP05, Theorem 1.4.5]

says that there is a positive number $m < 2\ln^2(p_1p_2) \leq 2\ln^2 n$ with $\chi_1(m) \neq 1$. Then $\chi_1(m) = 0$ or -1. If $\chi_1(m) = 0$, then m is divisible by p_1 or p_2, which implies that m is a witness. Suppose $\chi_1(m) = -1$, so that either $(m/p_1) = 1$, $(m/p_2) = -1$ or vice versa. Without loss of generality, assume the first holds. Then, as noted above, if (5.1) holds then $m^{2^{s_2-1}t} \equiv -1 \pmod{n}$, which in turn implies that $(m/p_1) = -1$, since $s_1 = s_2$. This contradiction shows that m is a witness for n. Now assume that $s_1 < s_2$. Again, [CP05, Theorem 1.4.5] implies that there is a natural number $m < 2\ln^2 p_2 < 2\ln^2 n$ with $(m/p_2) = \chi_2(m) \neq 1$. If $(m/p_2) = 0$, then m is divisible by p_2 and is a witness. If $(m/p_2) = -1$, then as above, m is not a witness implies $m^{2^{s_2-1}t} \equiv -1 \pmod{n}$. Then Lemma 5.16 implies that $2^{s_2}|p_1 - 1$, so that $s_2 \leq s_1$, a contradiction. Thus, m is a witness for n, and the proof is complete. □

[CP05, p.142] closes with the question what can be proved unconditionally. It is obvious that $W(n) \leq n^{1/2}$, since the least prime factor of an odd composite number n is a witness for n. In [Bur97] it is shown that $W(n) \leq n^{c+o(1)}$ as $n \to \infty$ through the odd composites, where $c = 1/(6\sqrt{e})$. Heath-Brown (see [BN97]) has recently shown this with $c = 1/10.82$.

The Miller-Rabin test shall be discussed now, but first some comments by [Rie94, p.91f] on strong primality tests will be reproduced. It will be taken into account that neither Euler pseudoprimes nor strong pseudoprimes admit the possibility of analogues to Carmichael numbers. Therefore, using Euler's criterion or a strong primality test with enough bases will finally reveal any composite number or, alternatively, prove the primality of any prime N. Some recent work by Gerhard Jaeschke [Jae93], shows that there exist only 101 numbers below 10^{12} which are strong pseudoprimes for all the bases 2, 3 and 5 simultaneously. Of these, only 9 will pass a strong primality test to base 7, and, finally, none of these is a strong pseudoprime to base 11. As a matter of fact, the smallest strong pseudoprime to all the bases 2, 3, 5, 7, and 11 simultaneously is the number 2 152 302 898 747, and thus 5 strong primality tests to these bases will prove a number below this limit prime (if it is). If we instead use the seven bases 2, 3, 5, 7, 11, 13, and 17, every number below 341 550 071 728 321 can be identified as prime or composite by this technique.- In practice we of course do not perform all seven tests first, and then decide on the character of the number. In most of the cases the test for base 2 already reveals the number as composed, and we are finished. If not, we pass on to the next test and so on.

This fact can be utilized to identify any number below $3.4 \cdot 10^{14}$ as being either composite or prime by means of the following very simple scheme:

1. Check whether N satisfies (5.1) for base 2. If not, then N is composite.
2. Check whether N satisfies (5.1) for base 3. If not, then N is composite.
3. If $N < 1373653$, then N is prime. If $N \geq 1373653$, check whether N satisfies (5.1) for base 5. If not, then N is composite.
4. If $N < \psi_3 = 25326001$, then N is prime. If $N \geq \psi_3$, check whether N satisfies (5.1) for base 7. If not, then N is composite.
5. If $N < \psi_4 = 3215031751$, then N is prime. If $N \geq \psi_4$, check whether N satisfies (5.1) for base 11. If not, then N is composite.
6. If $N < \psi_5 = 2152302898747$, then N is prime. If $N \geq \psi_5$, check whether N satisfies (5.1) for base 13. If not, then N is composite.
7. If $N < \psi_6 = 3474749660383$, then N is prime. If $\psi_6 \leq N < 341550071728321$, check whether N satisfies (5.1) for base 17. If not, then N is composite.

In [Jae93] Jaeschke also discusses the possibility of using bases other than the first primes for the strong primality tests. With suitable choices of the bases, the number of tests can be cut down. Thus he finds that four bases, viz. 2, 13, 23, and 1 662 803 will suffice to decide upon the primality of any number up to 10^{12}.
Recalling from [KLS01, p. 137f] it is proven in [Rab80, Mon80] that a composite odd integer $n > a$ can be a strong pseudoprime to the base a for at most $\phi(n)/4$ bases a such that $1 \leq a < n$ and $\gcd(a, n) = 1$. Thus, if the base a is chosen randomly, the probability that n is a strong pseudoprime to the base a is less than or equal to $\frac{1}{4}$. This gives rise to the Miller-Rabin probabilistic primality test, which improves the Solovay-Strassen primality test.

Or as it is expressed in [Rie94, p.92]: Using a number of strong primality tests with randomly chosen bases a is called the *Rabin-Miller probabilistic compositeness test.* It reveals the compositeness of most composites, but can never prove a number to be prime. Because as we have seen it is possible to construct composite numbers, which are strong pseudoprimes to any given, finite set of bases a.

In [FR07, p.224] it is written that the Miller-Rabin test now proceeds exactly as the Solovay-Strassen test, except that the probability now that n is prime is greater than $1 - \frac{1}{4^k}$.

A even more elaborate discussion of the Rabin-Miller test can be found in [CP05, p.137]. Since one can perform a strong pseudoprime test very rapidly, it is easy to

decide whether a particular number a is a witness for n. All said, it would seem that it is quite an easy task to produce witnesses for odd composite numbers. Indeed, it is, if one uses a probabilistic algorithm. The following is often referred to as "the Miller-Rabin test", though as one can readily see, it is algorithm 5.2 done with a random choice of the base a. (The original test in [Mil76] was somewhat more complicated and was a deterministic, ERH-based test. It was M. Rabin, see [Rab76, Rab80], who suggested a probabilistic algorithm as below.)

Algorithm 5.21. (**Random compositeness test**) *[CP05, p.137]*
We are given an odd number $n > 3$. This probabilistic algorithm attempts to find a witness for n and thus prove that n is composite. If a is a witness, (a, YES) is returned; otherwise, (a,NO) is returned.

1. (Choose possible witness)
   Choose random integer $a \in [2, n-2]$;
   Via algorithm 5.2 decide whether n is a strong probable prime base a;

2. (Declaration)
   if (n is a strong probable prime base a) return (a, NO);
   return (a, YES);

One can see from Theorem 5.14 that if $n > 9$ is an odd composite, then the probability that Algorithm 5.21 fails to produce a witness for n is $< 1/4$. No one is stopping us from using Algorithm 5.21 repeatedly. The probability that we fail to find a witness for an odd composite number n with k (independent) iterations of Algorithm 5.21 is $< 1/4^k$. So clearly we can make this probability vanishingly small by choosing k large. Algorithm 5.21 is a very effective method for recognizing composite numbers. But what does it do if we try it on an odd prime? Of course it will fail to produce a witness, since Theorem 5.1 asserts that primes have no witnesses.

Suppose n is a large odd number and we don't know whether n is prime or composite. Say we try 20 iterations of Algorithm 5.21 and fail each time to produce a witness. What should be concluded? Actually, nothing at all can be concluded concerning whether n is prime or composite. Of course, it is reasonable to strongly conjecture that n is prime. The probability that 20 iterations of Algorithm 5.21 fail to produce a witness for a given odd composite is less than 4^{-20}, which is less than one chance in a trillion. So yes, n is most likely prime. But it has not been proved prime and in fact might not be.

In [FR07, p.225] the Miller-Rabin test is presented in a different manner:

Algorithm 5.22. Miller-Rabin primality test
Input an odd integer n and suppose $n-1 = 2^s t$ with t odd.

1: Choose k random integers $b_1, \ldots, b_k$ with $1 < b_i < n$

2: For $i = 1, \ldots, k$

a: Compute $\gcd(b_i, n)$ (by the Euclidean algorithm)
i: If $\gcd(b_i, n) > 1$, then n is composite and stop

b: For $i = 1, \ldots, k$
i: Compute $m_i \equiv b_i^t \bmod n$,
j: If $m_i = \pm 1$, then n is a strong pseudoprime to the base b_i and go on to the next i. Else
k: For $j = 1, \ldots, s-1$ compute $k_j = b_i^{2^j t}$
l: If $k_j \equiv -1 \bmod n$, then n is a strong pseudoprime to the base b_i and go on to the next i. If not then go to the next j .
m: If k_j is not congruent to -1 mod n for all j , then n is composite and stop

3: The probability that n is prime is greater then $1 - \frac{1}{4^k}$

The Miller-Rabin test can be made deterministic under the assumption the the extended Riemann hypothesis holds.

5.3 Distribution and Infinitude

Like in the case of Fermat pseudoprimes and Euler pseudoprimes [Rib04, p.98] is citing Monier (1980) [Mon80], who has also determined a formula for the number $B_{\text{spsp}}(n)$ of bases a, $1 < a < n$, $\gcd(a, n) = 1$, for which the odd composite integer n is spsp(a). Namely:

$$B_{\text{spsp}}(n) = \left(1 + \frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1}\right) \left(\prod_{p|n} \gcd(n^*, p^*)\right) - 1,$$

where

$$\begin{aligned}
\omega(n) &= \text{number of distinct prime factors of } n,\\
\nu(n) &= \min_{p|n}\{v_2(p-1)\},\\
v_p(m) &= \text{exponent of } p \text{ in the factorization of } m\\
&\quad\ \text{(any natural number)},\\
m^* &= \text{largest odd divisor of } m-1
\end{aligned}$$

***Remark* 5.23.** *[KLS01, p.139]* Theorem 5.10, which is proved in [PSW80, p.1008], enables us to generate infinitely many strong pseudoprimes and hence by Theorem 5.8 also infinitely many Euler pseudoprimes in a simple manner.
Let F_m be a composite Fermat number. By Theorem 5.9, F_m is a strong pseudoprime. Applying Theorem 5.10 recursively, we can generate infinitely many strong pseudoprimes from one strong pseudoprime F_m.

[Rib04, p.97] notes that in 1980, Pomerance, Selfridge & Wagstaff [PSW80] proved that for every base $a > 1$, there exist infinitely many spsp(a). For base 2, it is possible to give infinitely many spsp(2) explicitly, as I indicate now. If n is a psp(2), then $2^n - 1$ is a spsp(2). Since there are infinitely many psp(2), this gives explicitly infinitely many spsp(2); among these are all composite Mersenne numbers. It is also easy to see that if a Fermat number is composite, then it is a spsp(2).

According to [Rib04, p.217] it is convenient to introduce the following notation for the counting functions of pseudoprimes, Euler and strong pseudoprimes in arbitrary bases $a \geq 2$:

$$\begin{array}{llll} P\pi_a(x) & = \#\{n | 1 \leq n \leq x,\ n \text{ is psp}(a)\}, & P\pi(x) & = P\pi_2(x), \\ EP\pi_a(x) & = \#\{n | 1 \leq n \leq x,\ n \text{ is epsp}(a)\}, & EP\pi(x) & = EP\pi_2(x), \\ SP\pi_a(x) & = \#\{n | 1 \leq n \leq x,\ n \text{ is spsp}(a)\}, & SP\pi(x) & = SP\pi_2(x). \end{array}$$

Clearly, $SP\pi_a(x) \leq EP\pi_a(x) \leq P\pi_a(x)$.
Concerning lower bounds, the best result to date is by Pomerance, in 1982 (see Remark 3 of his paper [Pom82]):

$$e^{(\log x)^\alpha} \leq SP\pi_a(x),$$

where $\alpha = 5/14$.

6 Superpseudoprimes

The content of this section is solely taken out of [KLS01, p.141*ff*].

6.1 Definition

Definition 6.1. *[KLS01, p.141]* A *superpseudoprime N to the base a* is a pseudoprime to the base a all of whose divisors greater than 1 are either primes or pseudoprimes to the base a; that is, if $d \mid N$, then

$$a^{d-1} \equiv 1 \pmod{d}.$$

Superspeudoprimes to the base 2 are simply called *superpseudoprimes*.

6.2 Properties

Below we give a necessary and sufficient condition for an odd composite integer N to be a superpseudoprime to the base a (see [Som04]).

Theorem 6.2. *[KLS01, p.141f] Let $p_1, p_2, \ldots, p_r$ be distinct odd primes and let $a \geq 2$ be such that $\gcd(a, p_i) = 1$ for every $i = 1, \ldots, r$. Suppose that p_i is a primitive prime divisor of $a^{t_i} - 1$ with multiplicity m_i for $1 \leq i \leq r$. We allow the possibility that $t_i = t_j$ for $1 \leq i < j \leq r$. Let*

$$h = \operatorname{lcm}(t_1, t_2, \ldots, t_r).$$

Let N be a composite integer such that

$$N = \prod_{i=1}^{r} p_i^{\ell_i},$$

where $1 \leq \ell_i \leq m_i$.
Then N is a superspeudoprime to the base a if and only if for each $i = 1, \ldots, r$ there exist an integer k_i such that

$$p_i = k_i h + 1. \tag{6.1}$$

Proof. Suppose (6.1) holds for $1 \leq i \leq r$. Let $d = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r}$ be a composite divisor of N, where $0 \leq g_i \leq \ell_i$ for $i = 1, \ldots, r$. To show that d is a pseudoprime to the base a, it suffices to establish that

$$\operatorname{ord}_d a | d - 1 \tag{6.2}$$

Since $p_i \equiv 1 \pmod{h}$ for $i = 1, \ldots, r$ by (6.1), we have $d \equiv 1 \pmod{h}$, or equivalently,

$$d - 1 \equiv 0 \pmod{h}. \tag{6.3}$$

Let e_i equal the order of a modulo $p_i^{g_i}$ for $i = 1, \ldots, r$. By Remark A.10.30, if $g_i \geq 1$, then $e_i = t_i$; otherwise, $e_i = 1$. Since $\gcd(p_i^{g_i}, p_j^{g_j}) = 1$ for $1 \leq i < j \leq r$, it follows that

$$\mathrm{ord}_d a = \mathrm{lcm}(e_1, e_2, \ldots e_r) | \mathrm{lcm}(t_1, t_2, \ldots t_r) = h \tag{6.4}$$

It now follows from (6.3) and (6.4) that (6.2) holds.
On the other hand, suppose N is a superpseudoprime to the base a and there exists a prime divisor p_i of N such that $p_i \not\equiv 1 \pmod{h}$ for some i, where $1 \leq i \leq r$. Then there exists a prime divisor q for which $q^m || h$, but $q^m \nmid p_i - 1$ for some positive integer m. By the definition of h, $q^m || t_j$ for some j such that $1 \leq j \leq r$. Since p_j is a primitive prime divisor of $a^{t_j} - 1$, we see by Lemma 12.21 in [KLS01] that $p_j \equiv 1 \pmod{t_j}$, which implies that

$$p_j \equiv 1 \pmod{q^m}.$$

We claim, however, that $p_i p_j$ is not a pseudoprime to the base a, contradicting the assumption that N is a superspeudoprime to the base a. Since $p_i \not\equiv 1 \pmod{q^m}$ and $p_j \equiv 1 (\mathrm{mod}\, q^m)$, we have $p_i p_j \not\equiv 1 (\mathrm{mod}\, q^m)$, i.e.,

$$p_i p_j - 1 \not\equiv 0 (\mathrm{mod}\, q^m).$$

Thus,

$$\mathrm{ord}_{p_j} a = t_j \nmid p_i p_j - 1$$

and a fortiori,

$$\mathrm{ord}_{p_i p_j} a \nmid p_i p_j - 1.$$

Hence, $p_i p_j$ is not a pseudoprime to the base a. □

***Remark* 6.3.** *[KLS01, p.142]* Using Theorem 6.2, we can easily construct superpseudoprimes from tables of primitive prime divisors of $2^n - 1$. For example, using the tables in [Rie94] or [BLS+88], we can generate the superpseudoprime $N = 89 \cdot 2113 \cdot 353 \cdot 2931542417$. That N is indeed a superspeudoprime follows because each of its four prime factors is congruent 1 modulo 88, the number 89 is a primitive prime divisor of $2^{11} - 1$, the number 2113 is a primitive prime divisor of $2^{44} - 1$, both 353 and 2931542417 are primitive prime divisors of $2^{88} - 1$, and $\mathrm{lcm}(11, 44, 88) = 88$.

Theorem 6.4 below, which appears in [Som04], gives a systematic method for producing superpseudoprimes. It is based on Theorem 6.2 and shows how the Fermat numbers can be used to generate infinitely many superpseudoprimes.

Theorem 6.4. *[KLS01, p.142f]*

(i) *If F_m is composite, then F_m is a superpseudoprime.*

(ii) *$F_m F_{m+1}$ is a superpseudoprime for all $m \geq 2$. In particular, there exist infinitely many superpseudoprimes.*

(iii) *Assumer that $m \geq 3$ and that each prime divisor of F_m is of the form $k2^{m+3}+1$, where k is a natural number. Then $F_m F_{m+1} F_{m+2}$ is a superpseudoprime with at least three distinct prime divisors.*

(iv) *Assume that $p_1, p_2, \ldots, p_s$ are any prime divisors of F_m such that $p_i \equiv 1 \pmod{2^{m+3}}$ for $1 \leq i \leq s$. Then $p_1 p_2 \cdots p_s F_{m+1} F_{m+2}$ is a superpseudoprime with at least three distinct prime divisors.*

(v) *If N is a pseudoprime with exactly two prime divisors, then N is a superpseudoprime.*

(vi) *If the Mersenne number M_p is composite, then M_p is a superpseudoprime.*

(vii) *Let $N = 2^t - 1$ be a composite integer with at least two primitive prime divisors. If $p_1, p_2, \ldots p_s$ are any primitive prime divisors of N, where $s \geq 2$ and repetitions are allowed up to the multiplicity of a primitive prime divisor, then $p_1 p_2 \cdots p_s$ is a superpseudoprime.*

(viii) *Let $t \geq 5$ be an odd integer and let $p_1, p_2, \ldots, p_s$ be any primitive prime divisors of $2^t - 1$, where $s \geq 1$, and let $q_1, q_2, \ldots, q_j$ be any primitive prime divisors of $2^{2t} - 1$, where $j \geq 1$. Repetitions are permitted for both the p's and q's up to the multiplicity of a primitive prime divisor. Then $p_1 p_2 \cdots p_s q_1 q_2 \cdots q_j$ is a superpseudoprime.*

(ix) *Suppose $8|t$. Let $p_1, p_2, \ldots, p_s$ be any primitive prime divisors of $2^t - 1$, where $s \geq 1$, and let $q_1, q_2, \ldots, q_j$ be any primitive prime divisors of $2^{2t} - 1$, where $j \geq 1$. Repetitions are permitted for both the p's and q's up to the multiplicity of a primitive prime divisor. Then $p_1 p_2 \cdots p_s q_1 q_2 \cdots q_j$ is a superpseudoprime.*

(x) *Any composite divisor d of a superpseudoprime is also a superpseudoprime.*

Proof. The assertions (i)-(x) follow from Theorem 6.2, Goldbach's Theorem A.7.20, Lucas's Theorem [KLS01, Theorem 6.1] , Remark A.10.30, Lemma[KLS01, Lemma 12.11], and Zsigmondy's Theorem [KLS01, Theorem 12.22] upon noting that if $8|t$, then $(\frac{2}{p}) = 1$ for any primitive prime divisor p of $2^t - 1$. □

***Remark* 6.5.** *[KLS01, p.143]* Parts (ii) and (iii) can be found in [Szy66]. The only known integers m for which $F_m F_{m+1} F_{m+2}$ is a superpseudoprime are $m = 3$, 4, and 8. In order to ascertain whether $F_{2,m}$ is a superpseudoprime we need to examine all the prime factors of F_m for $m \geq 3$ and check whether they are all of the form $k2^{m+3} + 1$. The only Fermat numbers F_m that have been factored completely are those for which $0 \leq m \leq 11$. Of these, we find in [KLS01, Appendix A] that the only F_m for which $m \geq 3$ and all of its prime factors are of the proper form are the primes F_3 and F_4 an the composite F_8.
By using part (iv) rather than part (iii) of Theorem 6.4, we can find many more superpseudoprimes with at least three distinct prime divisors.
By Schinzel's Theorem [KLS01, Theorem 12.23], part (vii) holds for any integer t such that $t \geq 28$ and $t \equiv 4 \pmod 8$.
Part (v) of Theorem 6.4 provides examples of superpseudoprimes N that are products of exactly two primes. These examples are not very interesting, since then the only proper divisors of N greater than 1 are primes. If we knew that there exist infinitely many composite Fermat numbers, then the superpseudoprimes $F_m F_{m+1}$ given in part (ii) of Theorem 6.4 would provide infinitely many superpseudoprimes with at least three prime divisors.

The next theorem (see [Som04]) uses Fermat numbers to generate infinitely many superpseudoprimes that are product of at least three distinct prime divisors.

Theorem 6.6. *[KLS01, p.143f] Let p be a primitive divisor of F_m, where $m \geq 3$. Then $(p-1)/2 > 2^{m+1}$. Let $p_1, p_2, \ldots, p_s$ be distinct primitive prime divisors of $2^{(p-1)/2} - 1$ and let $q_1, q_2, \ldots, q_j$ be distinct primitive prime divisors of $2^{p-1} - 1$, where $j, s \geq 1$. Then $N = pp_1p_2 \cdots p_s q_1 q_2 \cdots q_j$ is a superpseudoprime with at least three distinct prime divisors. In particular, there exist infinitely many superpseudoprimes with at least three distinct primitive prime divisors.*

Proof. By Remark A.10.30, p is a primitive prime divisor of $2^{2^{m+1}} - 1$. By Zsigmondy's Theorem [KLS01, Theorem 12.22], each of the terms $2^{2^{m+1}} - 1$, $2^{(p-1)/2} - 1$, and $2^p - 1$ has primitive prime divisors. By Theorem [KLS01, Theorem 6.7], if F_m is composite, then the prime divisor p of F_m is of the form $k2^{m+2} + 2$ whether F_m is prime or composite. However, we observe that $p \equiv 1 \pmod{16}$, and therefore we obtain $(p - 1)/2 \equiv 0 \pmod 8$. According to [KLS01, Lemma 12.21 (i)], any primitive prime divisor of $2^{(p-1)/2} - 1$ is congruent to 1 modulo 8. Let p_i, $i \in \{1, \ldots, s\}$, be a primitive prime divisor of $2^{(p-1)/2} - 1$. Then $(\frac{2}{p_i}) = 1$, and using [KLS01, Lemma 12.21 (ii)] again, we see that $p_i \equiv 1 \pmod{2(p-1)/2}$, i.e.,

$$p_i \equiv 1 \pmod{p-1}.$$

Thus, each of the distinct primes $p, p_1, p_2, \ldots, p_s, q_1, q_2, \ldots, q_j$ is congruent to 1 (mod $p-1$). Since

$$2^{m+1} | p - 1,$$

it follows by Theorem 6.2 that the number N is a superpseudoprime. The theorem is thus proved. □

***Remark* 6.7.** *[KLS01, p.144]* Since any composite divisor of a superpseudoprime is also a superpseudoprime by Theorem 6.1 (x), [KLS01, Theorem 12.28] implies that there exist infinitely many superpseudoprimes with exactly three distinct prime divisors. The papers [Szy65], [Rot68], [FK83], and [Som04] provide other infinite classes of superpseudoprimes to the base a with exactly three distinct prime divisors.

A Appendix - Preliminaries from Number Theory

A.1 Congruences

"Congruence is related to the notion of divisibility"[Chi09, p.71].

Definition A.1.1. *[Chi09, p.71]* Two integers a and b are *congruent modulo* m, written

$$a \equiv b \pmod{m} \tag{A.1}$$

if m divides $a - b$, or equivalently, if $b = a+$ some multiple of m. A special case is that a number a is congruent to $0 \pmod{m}$, written $a \equiv 0 \pmod{m}$, if and only if m divides a. But the value of the congruence notation is not in providing an alternate for the notation $m|a$, but in providing a highly suggestive notation to use in place of $m|(a - b)$.
In a congruence $\pmod{m}$, the number m is called the modulus. Any two integers are congruent modulo 1, so the modulus 1 is not of much interest. For this reason the modulus will normally be ≥ 2.

Proposition A.1.2. *[Chi09, p.74] Congruence modulo m is:*
Reflexive: $a \equiv a \pmod{m}$ for all integers a;
Symmetric: for all integers a, b, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;
Transitive: for all integers a, b, c, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Lemma A.1.3. *[KLS01, p.14] If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then we also have*

$$ac \equiv bd \pmod{m} \tag{A.2}$$

Proof. Indeed, if $a = b + im$ and $c = d + jm$, then $ac = db + (jb + id + ijm)m$, and congruence (A.2) follows. □

A.2 Chinese Remainder Theorem

As it is written in [FR07, p.37], a linear congruence is of the form $ax+b \equiv 0 \pmod{m}$, where $a \not\equiv 0 \pmod{m}$.

Theorem A.2.4. ***(Chinese remainder theorem)*** *[FR07, p.40]*
Suppose that $m_1, m_2, \ldots, m_k$ are k positive integers that are relatively prime in pairs. If $a_1, \ldots, a_k$ are any integers then the simultaneous congruences

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \ldots, k,$$

have a common solution that is unique modulo $m_1 m_2 \ldots m_k$.

Proof. The proof we give not only provides a verification but also provides a technique for finding the common solution.
Let $m = m_1 m_2 \ldots m_k$. Since the m_i are relatively prime in pairs we have $\gcd(\frac{m}{m_i}, m_i) = 1$. Therefore there is a solution x_i to the reduced congruence

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}$$

Further, for x_i we clearly have

$$\frac{m}{m_i} x_i \equiv 0 \pmod{m_j} \qquad \text{if } i \neq j.$$

Now let

$$x_0 = \sum_{i=1}^{k} \frac{m}{m_i} x_i a_i.$$

We claim that x_0 is a solution to the simultaneous congruences and that it is unique modulo m. Now,

$$x_0 = \sum_{i=1}^{k} \frac{m}{m_i} x_i a_i \equiv \frac{m}{m_j} x_j a_j \pmod{m_j}$$

since $\frac{m}{m_i} x_i \equiv 0 \pmod{m_j}$ if $i \neq j$. It follows then that

$$x_0 \equiv \frac{m}{m_j} x_j a_j \equiv a_j \pmod{m_j}$$

since $\frac{m}{m_j} x_j \equiv 1 \pmod{m_j}$. Therefore x_0 is a common solution. We must prove the uniqueness part.
If x_1 is another common solution then $x_1 \equiv x_0 \pmod{m_i}$ for $i = 1, \ldots, k$. Therefore $x_1 \equiv x_0 \pmod{m}$.
We note that if the integers m_i are not relatively prime in pairs there may be no solution to the simultaneous congruences. □

A.3 Legendre Symbol

Definition A.3.5. *[KLS01, p.23]* Let $n \geq 2$ and a be integers such that $\gcd(a, n) = 1$. If the quadratic congruence

$$x^2 \equiv a \pmod{n}$$

has a solution x, then a is called a *quadratic residue modulo n*. Otherwise, a is called a *quadratic nonresidue modulo n*.

Definition A.3.6. *[Chi09, p.437]* Let p be an odd prime, and a any number not divisible by p. Then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\begin{aligned}
&\left(\frac{a}{p}\right) = 1 && \text{if } a \text{ is a quadratic residue} \mod p,\\
&\left(\frac{a}{p}\right) = -1 && \text{if } a \text{ is a quadratic nonresidue} \mod p,\\
\text{and we define explicitly } &\left(\frac{a}{p}\right) = 0 && \text{for the special case } p|a.
\end{aligned}$$

To decide whether a is square modulo p, we can manipulate Legendre symbols with following rules:

Theorem A.3.7. *[Chi09, p.437] Assume p, q are distinct odd primes and a and b are integers coprime to p. Then*

$$\begin{aligned}
&(1)\quad \left(\frac{a^2}{p}\right) = 1; && (4)\quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};\\
&(2)\quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \text{ if } a \equiv b \pmod{p}; && (5)\quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};\\
&(3)\quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right); && (6)\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.
\end{aligned}$$

Definition A.3.8 (Jacobi symbol - Extension of the Legendre symbol)**.** *[FR07, p.221]* If n is a positive odd integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ and a is a positive integer then the Jacobi symbol is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k} \tag{A.3}$$

(Several of the results concerning the Legendre symbol, including quadratic reciprocity, can be extended to the Jacobi symbol.)

A.4 Euler's Criterion

Theorem A.4.9. *(**Euler's Criterion**) [KLS01, p.23f]*
Let p be an odd prime. Then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{A.4}$$

Proof. If $p \mid a$, then (A.4) is clearly satisfied. Now suppose that $p \nmid a$. By Fermat's Little Theorem A.5.10,

$$a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p}. \tag{A.5}$$

Since p is prime, either $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$. It thus suffices to prove that $a^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if a is a quadratic residue modulo p.
Let a be a quadratic residue modulo p; i.e., $a \equiv b^2 \pmod{p}$ for some integer b such that $b \not\equiv 0 \pmod{p}$. Then by Fermat's little theorem,

$$a^{(p-1)/2} \equiv \left(b^2\right)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Conversely, assume that $a^{(p-1)/2} \equiv 1 \pmod{p}$. Let q be a primitive root modulo p. Then $a \equiv q^t \pmod{p}$ for some t such that $1 \leq t \leq 1 - p$. Then

$$q^{t(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

However, $\mathrm{ord}_p q = p - 1$, and hence $p - 1 \mid t(p-1)/2$. This implies that $2 \mid t$, so let $t = 2j$. Then $(q^j)^2 = q^t \equiv a \pmod{p}$ and $\left(\frac{a}{p}\right) = 1$. □

A.5 Fermat's Little Theorem

It is a special case of Euler's theorem (see Section A.4).

Theorem A.5.10. *(**Fermat's little Theorem**) [KLS01, p.16]*
If a is a natural number and p a prime number, then $p \mid a^p - a$.

Proof. If $p \mid a$, then p also divides $a^p - a = a(a^{p-1} - 1)$. So let

$$\gcd(p, a) = 1. \tag{A.6}$$

We will show that then $p \mid a^{p-1} - 1$. Consider the finite sequence

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a,\ pa. \tag{A.7}$$

Dividing the two numbers ia and ja, $1 \leq j < i \leq p$, by p, we cannot obtain the same

remainder, since then $p \mid a(i-j)$, which contradicts (A.6). Hence, the sequence (A.7) yields p different remainders upon division by p. Le us remove the last term in (A.7), which produces the remainder 0. We obtain the same remainders (up to order) when dividing the sequence $1, \ldots, p-1$ by p. From this and by induction using (A.2), we arrive at $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Consequently,

$$(a^{p-1}-1)(p-1)! \equiv 0 \pmod{p}$$

and the first term on the left-hand side is thus divisible by the prime p, since $p \nmid (p-1)!$ □

***Remark* A.5.11.**

(i) *[KLS01, p.17]* Fermat's little theorem is often formulated by means of the congruence notation as follows:
If p is a prime and a is a natural number coprime to p, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{A.8}$$

Congruence (A.8) can be used to prove that a given number is composite without knowing any of its factors. Namely, if we find a "small" a satisfying (A.6) such that (A.8) does not hold, then p is not a prime.

(ii) *[KLS01, p.130]* We will make use of Fermat's little Theorem in either of its two equivalent forms. The first form states that if p is a prime, then

$$a^{p} \equiv a \pmod{p} \tag{A.9}$$

for all integers a. The second form states that if p is a prime and $\gcd(a,p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{A.10}$$

However, the converse of Fermat's little theorem is not true. Given any base $a > 1$, there exists a composite integer n coprime to a such that

$$a^{n} \equiv a \pmod{n}. \tag{A.11}$$

(iii) *[KLS01, p.131]* If $\gcd(a,n) = 1$, then (A.11) holds if and only if

$$a^{n-1} \equiv 1 \pmod{n}. \tag{A.12}$$

A.6 Carmichael lambda function and Euler totient function

Definition A.6.12. *[KLS01, p.21]* Let n be a positive integer. Then the *Carmichael lambda function* $\lambda(n)$ is defined as follows:

$$\begin{aligned}
\lambda(1) &= 1 = \phi(1),\\
\lambda(2) &= 1 = \phi(2),\\
\lambda(4) &= 2 = \phi(4),\\
\lambda(2^k) &= 2^{k-2} = \frac{1}{2}\phi(2^k) \quad \text{for } k \geq 3,\\
\lambda(p^k) &= (p-1)p^{k-1} = \phi(p^k) \quad \text{for any odd prime } p \text{ and } k \geq 1,\\
\lambda(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}) &= \operatorname{lcm}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots \lambda(p_r^{k_r})),
\end{aligned}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $k_i \geq 1$ for $1 \leq i \leq r$.

[KLS01, p.19] further introduces the *Euler totient function* ϕ. For every $n \in \mathbb{N}$ the value $\phi(n)$ is defined as the number of all natural numbers not greater than n that are coprime to n, i.e., $\phi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m,n) = 1\}|$ where $|.|$ denotes the number of elements. We can easily find that

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(5) = 4, \quad \phi(6) = 2, \quad \phi(7) = 6, \ldots$$

and that all other values of ϕ are even. If p is prime, then clearly

$$\begin{aligned}
\phi(p) &= p - 1 \qquad &&\text{and}\\
\phi(p^k) &= (p-1)p^{k-1} \qquad &&\text{for every } k \in \mathbb{N}.
\end{aligned}$$

Another interesting property of the Euler totient function can be expressed as follows:

$$\gcd(m,n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n).$$

And let us recall Gauss's well-known formula

$$\sum_{d|N} \phi(d) = N \qquad \forall N \in \mathbb{N}.$$

Theorem A.6.13. ***(Carmichael's Theorem)*** *[Rie94, p.274]*
If $\gcd(a,n) = 1$, *then*

$$a^{\lambda(n)} \equiv 1 \pmod{n}. \tag{A.13}$$

(This is a very useful, but often forgotten generalization of Euler's Theorem.)

A.7 Fermat Numbers

Definition A.7.14. *[KLS01, p.1]* Let $m \in \mathbb{N}$ (meaning $0 \in \mathbb{N}$) then the numbers

$$F_m = 2^{2^m} + 1 \tag{A.14}$$

are called *Fermat numbers.*

***Remark* A.7.15.** *[KLS01, p.1]* Pierre de Fermat became well known not only due to Fermat's last theorem and Fermat's little theorem, but also due to the conjecture that all numbers F_m are prime. In 1732 Leonhard Euler found that $F_5 = 641 \cdot 6700417$, and thus disproved the Fermat conjecture.
Then a natural question arose, whether there exist infinitely many prime numbers of the form (A.14). If F_m is prime, we say the it is a Fermat prime. The first five members of sequence (A.14), i.e.,

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

are primes.

Proposition A.7.16. *[KLS01, p.26] The formula*

$$F_{m+1} = F_m + 2^{2^m} F_0 F_1 \cdots F_{m-1} \tag{A.15}$$

holds for all $m \geq 1$.

Proof. We have

$$F_{m+1} - F_m = 2^{2^{m+1}} + 1 - 2^{2^m} - 1 = 2^{2^m} \left(2^{2^m} - 1\right). \tag{A.16}$$

However,

$$2^{2^m} - 1 = \left(2^{2^{m-1}} - 1\right)\left(2^{2^{m-1}} + 1\right) = \left(2^{2^{m-1}} - 1\right) F_{m-1}.$$

By induction, we get easily that

$$2^{2^m} - 1 = \left(2^{2^{m-k}} - 1\right) F_{m-k} F_{m-k+1} \cdots F_{m-1} \qquad \text{for all } k \in \{1, \ldots, m\}.$$

In particular, when $k = m$, we get

$$2^{2^m} - 1 = F_0 F_1 \cdots F_{m-1}. \tag{A.17}$$

Now formula (A.15) is an immediate consequence of formulae (A.16) and (A.17). □

Proposition A.7.17. *[KLS01, p.26f] The formula*

$$F_m = F_0 F_1 \cdots F_{m-1} + 2 \tag{A.18}$$

holds for all $m \geq 1$.

Proof. For $m \geq 1$, we use formula (A.17) and get

$$F_m - 2 = \left(2^{2^m} + 1\right) - 2 = 2^{2^m} - 1 = F_0 F_1 \cdots F_{m-1},$$

which is exactly formula (A.18). □

***Remark* A.7.18.** *[KLS01, p.27]* Notice that Proposition A.7.17 implies that $F_m - 2$ for $m \geq 1$ is divisible by all the smaller Fermat numbers; that is,

$$F_k \,|\, F_m - 2 \quad \text{for all } k = 0, 1, \ldots, m-1,$$

or equivalently,

$$F_m \equiv 2 \pmod{F_k} \quad \text{for all } k = 0, 1, \ldots, m-1. \tag{A.19}$$

Lemma A.7.19. *[KLS01, p.36] For any* $n \leq 2^m - 1$ *we have* $F_m \,|\, 2^{F_m} - 2$.

Proof. We see that

$$2^{F_m} - 2 = 2\left(2^{2^{2^m}} - 1\right) = 2\left(2^{2^{2^m}} + 1 - 2\right) = 2\left(F_{2^m} - 2\right) = 2F_0F_1F_2 \ldots F_{2^m-1},$$

where the last equality follows from recurrence (A.18). □

Theorem A.7.20. *(**Goldbach's Theorem**)[KLS01, p.33]*
No two different Fermat numbers have a common divisor greater than 1.

Proof. Assume that

$$q \,|\, F_m \qquad \text{and} \qquad q \,|\, F_{m-k} \tag{A.20}$$

for $m \geq k \geq 1$. From this and (A.19) we obtain $q \,|\, F_m - 2$. Hence, according to (A.20), we see that $q \,|\, 2$. However, since F_m is odd, we get $q = 1$. □

Theorem A.7.21. *[KLS01, p.37] Let* $q = p^n$ *be a power of an odd prime* p, *where* $n \geq 1$. *Then the Fermat number* F_m *is divisible by* q *if and only if*

$$\operatorname{ord}_q 2 = 2^{m+1}.$$

Proof. Suppose that $q \,|\, F_m$. Then q obviously also divides the number $2^{2^{m+1}} - 1 = \left(2^{2^m} + 1\right)\left(2^{2^m} - 1\right)$. From this and Lemma A.10.27 for $a = 2$ it follows that $\operatorname{ord}_q 2 \leq$

2^{m+1} and $2^{m+1} = k\text{ord}_q 2$ for some $k \in \mathbb{N}$. Thus, k has to be a power of 2 and $e = \text{ord}_q 2 = 2^j$. However, if j were less than $m+1$. then by Lemma A.10.27, the number

$$2^{e2^{m-j}} - 1 = 2^{2^m} - 1$$

would be divisible by the odd number $q > 1$, which contradicts the assumption $q \,|\, F_m$. Therefore, $\text{ord}_q 2 \geq 2^{m+1}$.
Conversely, assume that $\text{ord}_q 2 = 2^{m+1}$. Then

$$q \,|\, 2^{2^{m+1}} - 1 = \left(2^{2^m} + 1\right)\left(2^{2^m} - 1\right).$$

Since p is odd and $p > 1$, the prime p, and thus also the prime power q, divides at most one of the numbers $2^m + 1$ and $2^m - 1$. But $q \nmid 2^{2^m} - 1$, since then $\text{ord}_q 2 \leq 2^m$. Thus,

$$q \,|\, 2^{2^m} + 1 = F_m$$

□

***Remark* A.7.22.** *[KLS01, p.37]* We get by completely similar arguments to those in the proof of Theorem A.7.21 that if $d > 1$ is any divisor of F_m (not necessarily prime; see also [Kel91]), then

$$\text{ord}_d 2 = 2^{m+1},$$

where the symbol $\text{ord}_d 2$ is defined in the same way as in Definition A.10.26. In particular,

$$\text{ord}_{F_m} 2 = 2^{m+1}.$$

A.8 Mersenne Numbers

Definition A.8.23. *[KLS01, p.213]* The number $M_p = 2^p - 1$, where p is prime, is called a *Mersenne number*. If $2^p - 1$ itself is a prime, the it is called *Mersenne prime*.

[Chi09, p.208*ff*] states that Mersenne conjectured in 1644 that $2^p - 1$ was prime for the following p: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257, and composite for the other primes $p > 257$. This conjecture turned out to be quite inaccurate above 31 ($2^p - 1$ is prime for p = 61,89,107, and 127, and composite for the other primes p with $31 < p \leq 257$). However, other Mersenne numbers, numbers of the form $2^p - 1$ for p prime and $p > 257$ have been found that are prime. This set of Mersenne primes includes some very large primes. There are several reasons why Mersenne numbers have been singled out for primality testing. One is because if we seek a prime number that is "almost" a power, then we are forced to look only at Mersenne numbers:

Proposition A.8.24. *[Chi09, p.208] If a number of the form $a^n - 1$ is prime, then $a = 2$ and n is prime.*

It is also mentioned in [KLS01, p.167*ff*] that there is a more general notion of Fermat numbers. These are called generalized Fermat numbers and they generalize both the Fermat numbers $F_m = L_{2,m}$ and the Mersenne numbers $M_p = L_{p,0}$.

Definition A.8.25. *[KLS01, p.167]* For p prime, $a \geq 2$, and $m \geq 0$ the generalized Fermat numbers are defined as

$$L_{p,m} = \frac{a^{p^{m-1}}-1}{a^{p^m}-1}$$

In this thesis they occur in the special form $F_{a,m} = L_{2,m}(a) = a^{2^m} + 1$. For more information on generalized Fermat numbers see [KLS01, Chapter 13].

A.9 Arithmetic Progression and Linnik's Constant

The two following short notes on these issues can be found in [Rib04, p.207].
With $d \geq 2$ and $a \geq 1$, relatively prime, let $p(d, a)$ be the smallest prime in the arithmetic progression $\{a + kd | k \geq 0\}$. Can one find an upper bound, depending only on a, d, for $p(d, a)$? Let $p(d) = \max\{p(d, a) | 1 \leq a < d, gcd(a, d) = 1\}$. Again, can one find an upper bound for $p(d)$ depending only on d? And how about lower bounds?
Linnik's theorem of 1944, which is one of the deepest results in analytic number theory asserts: There exists $d_0 \geq 2$ and $L > 1$ such that $p(d) < d^L$ for every $d \geq d_0$.
Note that the absolute constant L, called Linnik's constant, is effectively computable. It is clearly important to compute the value of L. Pan Cheng-Dong was the first to evaluate Linnik's constant, giving $L \geq 5448$ in 1957. Subsequently, a number of papers have appeared, where the estimate of the constants was improved.

A.10 Multiplicative Order, Primitive Root, and Primitive Prime Divisor

Definition A.10.26. *[KLS01, p.17]* Let d and a be positive integers such that $\gcd(d, a) = 1$. The smallest positive exponent e for which $d \mid a^e - 1$ (i.e., $a^e \equiv 1 \pmod{d}$) is called the *multiplicative order of the number a modulo d*, which we shall write as $e = \mathrm{ord}_d a$.

Lemma A.10.27. *[KLS01, p.17] If $e = \mathrm{ord}_d a$, then $d \mid a^n - 1$ for $n = ke$, $k \in \{1, 2, \dots\}$, and the relation holds only for these exponents.*

Proof. If $n = ke$, then

$$a^n - 1 = a^{ke} - 1 = (a^e - 1)\left(a^{e(k-1)} + \cdots + a^e + 1\right),$$

and thus the $d \mid a^n - 1$ is valid due to the previous definion A.10.26.
Assume, for instant, that $d \mid a^{ke+h} - 1$ for some $k \in \{1, 2, \dots\}$ and $0 < h < e$. Then

$$\left(a^{ke+h} - 1\right) - \left(a^{ke} - 1\right) = a^{ke}\left(a^h - 1\right).$$

Since both the numbers in parentheses on the left are divisible by d and, by $d \mid a^n - 1$, $\gcd(d, a^{ke}) = 1$, we get that $a^h - 1$ is divisible by d. This contradicts the minimality of e. □

Definition A.10.28. *[KLS01, p.18]* Let p be a prime. By Fermat's little theorem, the maximum order modulo p of any integer a coprime to p is $p - 1$. We call the integer $g \not\equiv 0 \pmod{p}$ a *primitive root modulo p* if $\mathrm{ord}_p g = p - 1$.

Definition A.10.29. *[KLS01, p.139]* Let a and b be coprime integers with $|a| > |b| \geq 1$ and let $n \geq 1$ be a positive integer. A prime p is called a *primitive prime divisor* of $a^n - b^n$ if $p \mid a^n - b^n$, but $p \nmid a^m - b^m$ for $1 \leq m < n$. Primitive prime divisors of $a^n + b^n$ are defined similarly.

***Remark* A.10.30.** *[KLS01, p.139]*

(i) It follows from relation (1.8) that p is a primitive prime divisor of $a^n - b^n$ if and only if $p \nmid a^d - b^d$ for any proper divisor d of n.

(ii) We make the following observation about primitive prime divisors. If p is a primitive prime divisor of $a^n - 1$ with multiplicity m, then, for $1 \leq i \leq m$,

$$\mathrm{ord}_{p^i} a = n. \tag{A.21}$$

Furthermore, every prime divisor of the Fermat number $F_m = 2^{2^m} + 1$ is a primitive prime divisor of $2^{2^{m+1}} - 1$.

B Appendix - Preliminaries from Analytic Number Theory

B.1 Dirichlet characters and series

Definition B.1.1. *[FR07, p.105]* For any integer k, a *Dirichlet character* modulo k is a complex valued function on the integers $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

(1) $\chi(a) = 0$ if $\gcd(a, k) > 1$,

(2) $\chi(1) = 1$,

(3) $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$ for all $a_1, a_2 \in \mathbb{Z}$,

(4) $\chi(a_1) = \chi(a_2)$ whenever $a_1 \equiv a_2 \pmod{k}$.

[FR07, p.105] continues as follows. From (3) and (4) it is clear that a Dirichlet character can be considered as a multiplicative complex function on the set of residue classes modulo k. We will shorten the notation and use the word character to mean a Dirichlet character modulo k.
From a group-theoretical point of view a Dirichlet character is just a character of a finite complex representation of the unit group $U(\mathbb{Z}_k)$. We will say more about this after our discussion of characters.
As an example consider the function

$$\chi_0(a) = \begin{cases} 0 & \text{if } \gcd(a, k) > 1, \\ 1 & \text{if } \gcd(a, k) = 1. \end{cases}$$

It is easy to verify that this is a character. Thus, modulo k, there is always at least one character. The character above is called the principal character and exists as defined for each k.
We now describe some necessary properties of characters. In each of the following results, when we say character we mean character modulo k, with k fixed.

Lemma B.1.2. *[FR07, p.106]*

(1) For every character, $\chi(1) = 1$.

(2) For every character, if $\gcd(a, k) = 1$ *then* $|\chi(a)|^{\phi(k)} = 1$. *Hence* $|\chi(a)| = 1$ *and* $\chi(a)$ *is a* $\phi(k)$*th root of unity.*

Proof. cf. [FR07, p.106] □

Lemma B.1.3. *[FR07, p.106] For every k there exist only finitely many characters mod k.*

Proof. cf. [FR07, p.106] □

Lemma B.1.4 (p.106)**.** *Fine2007*

(1) If χ_1 and χ_2 are characters, then so is $\chi_1\chi_2$, where $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$.

(2) If χ is a character, so is its complex conjugate $\overline{\chi}$. Further, $\chi(a)^{-1} = \overline{\chi(a)}$.

(3) If χ_1 is a fixed character and χ runs over all characters, then so does $\chi_1\chi$.

Proof. cf. [FR07, p.106] □

Lemma B.1.5. *[FR07, p.106] If $d > 0$ and $\gcd(d, k) = 1$ with d not congruent to 1 (mod k), then there exists a character for which $\chi(d) \neq 1$.*

Proof. cf. [FR07, p.107] □

For the time being we will let c denote the finite number of characters modulo k. After we prove certain orthogonality relations we will show that $c = \phi(k)$.

Theorem B.1.6 (**orthogonality relations I**)**.** *[FR07, p.108]*

(1) If χ is a fixed character and a runs over a complete set of residue classes mod k, then

$$\sum_a \chi(a) = \begin{cases} \phi(k) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(2) If $a > 0$ is an integer, then if χ runs over the set of all c characters,

$$\sum_\chi \chi(a) = \begin{cases} c & \text{if } a \equiv 1 \pmod{k}, \\ 0 & \text{if } a \not\equiv 1 \pmod{k}. \end{cases}$$

Proof. cf. [FR07, p.108f] □

Corollary B.1.7. *[FR07, p.109] There exist exactly $\phi(k)$ characters modulo k.*

Proof. cf. [FR07, p.109] □

Theorem B.1.8 (orthogonality relations II). *[FR07, p.109]*

(1) If χ_1 and χ_2 are character mod k and a runs over a complete set of residue classes mod k, then

$$\sum_a \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \phi(k) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

(2) If $a > 0$ is an integer, then if χ runs over the set of all c characters,

$$\sum_\chi \chi(t)\overline{\chi(a)} = \begin{cases} \phi(k) & \text{if } a \equiv t \pmod{k}, \\ 0 & \text{if } a \not\equiv t \pmod{k}. \end{cases}$$

Proof. cf. [FR07, p.110] □

Definition B.1.9. *[FR07, p.110]* If χ is a character mod k then the *Dirichlet L-series* is defined for complex values s by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Theorem B.1.10. *[FR07, p.111] For any character χ mod k the Dirichlet L-series is an analytic function for* $\mathrm{Re}\, s > 1$. *Further, it has an Euler product representation*

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

The proof of this theorem and some properties of Dirichlet L-series can be found in [FR07, p.111-121].

B.2 Riemann Hypothesis

Definition B.2.11. *[FR07, p.134]* For a $\operatorname{Re} s > 1$ we define the *Riemann zeta function* by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Some statements on the Riemann zeta function can be found in [FR07, p.166*ff*]. According to [FR07, p.135] in 1859 Riemann attempted to give a complete proof of the prime number theorem using the zeta function for a complex variable s. Although he was not successful in proving the prime number theorem, he established many properties of the zeta function and showed that the prime number theorem depended on the zeros of the zeta function. He conjectured that all the zeros of $\zeta(s)$ in the strip $0 \leq \operatorname{Re}(s) \leq 1$ lie along the line $\operatorname{Re}(s) = \frac{1}{2}$. This is known as the Riemann hypothesis and is still an open problem. Furthermore in [FR07, p.170] it is noted, that what becomes crucial in applying the zeta function to the proof of the prime number theorem is the location of its zeros. In particular the fact that $\zeta(s)$ has no zeros on the line $\operatorname{Re}(s) = 1$ is equivalent to the prime number theorem.
In [FR07, p.191] there is also mentioned one major extension of the Riemann hypothesis, which is assumed in section 5 in theorem 5.20.

Conjecture B.2.12 (**Extended Riemann Hypothesis (ERH)**). *[FR07, p.191] For an integer k and any character χ mod k, the nontrivial zeros of the L-series*

$$L(x, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

all lie along the critical line $\operatorname{Re}(s) = \frac{1}{2}$.

C Appendix - Preliminaries from Cryptography

C.1 Public-Key Cryptography

[Chi09, p.404] introduces Alice, Bob and Eve. Alice and Bob wish to communicate privately. Eve can see everything sent between Alice and Bob. Alice and Bob don't want Eve to be able to read messages from Alice to Bob, so need to encrypt the messages so that Eve cannot read them. In their celebrated paper, W. Diffie and M. Hellman (1976) introduced the idea of a public key cryptosystem. They presented a method by which Alice and Bob can obtain a common private key, and in order for Eve to know the key, Eve would apparently have to solve the discrete logarithm problem. Diffie and Hellman's scheme solves the problem of communicating a private key through a public channel. The scheme works as follows. Alice and Bob agree on a finite cyclic group G of large order, and a generator g of G. The shared key will be an element of G. Alice chooses a random number a between 0 and the order of G, computes $g^a = A$ in G and sends the resulting group element A to Bob, while keeping the exponent a secret. Bob chooses a random number b between 0 and the order of G, computes $g^b = B$ in G and sends the resulting group element B to Alice, while keeping the exponent b secret. Alice and Bob's shared private key is then $K = g^{ab}$ in G. Alice can compute K by computing $B^a = (g^b)^a$, which she can do because she knows a and she received B from Bob. Bob can compute K by computing $A^b = (g^a)^b$, which he can do because he knows b and he received A from Alice. Assume that Eve can eavesdrop on the transmissions between Alice and Bob. Then Eve knows G, g, A and B. She wants to learn the key K. Since $K = A^b = B^a = g^{ab}$, she can determine K if she can learn a or b or ab. We can state Eve's problem as follows:
Diffie-Hellman problem: Given a group G, an element g in G, and elements A and B in $\langle g \rangle$ where $A = g^a$ for some unknown number a and $B = g^b$ for some unknown number b, determine $K = g^{ab}$ in G.

C.2 RSA-Algorithm

According to [Chi09, p.200] Euler's theorem is the key result behind the widely used RSA cryptosystem, developed by R.L. Rivest, A. Shamir, and L. Adleman (1977). Suppose two parties, call them Alice and Bob, wish to send messages back and forth to each other, and want them to be incomprehensible to a third party, say Eve. The idea is to encrypt each message, to transform the plaintext message into a message that would be unreadable except to the intended receiver. Even if the encrypted message is broadcast publicly, or sent over the internet, Eve, reading the encrypted message, should not be able to determine in a reasonable amount of time what the original

message is. Any message in words can be translated into a sequence of numbers by replacing the letters of the message by numbers in some agreed-upon way. For example, we could count the alphabet and replace each letter by the corresponding two-digit number.

How RSA works. For Alice to send Bob a message, Bob chooses two different large primes p and q that he keeps secret, and sets $m = pq$. He chooses an encrypting exponent e coprime to $\varphi(m) = (p-1)(q-1)$. Then Bob finds a number d so that

$$ed \equiv 1 \pmod{\phi(m)}.$$

Then d is the inverse of e modulo $\phi(m)$. Bob can find d by solving the equation

$$ex + \phi(m)y = 1$$

for x. Since e and $\phi(m)$ are coprime, Bob can solve this equation efficiently by the extended Euclidean Algorithm [Chi09, (Bezout's Identity) Section 3D]. Thus

$$ed = 1 + \phi(m)k$$

for some k. Bob keeps d secret but broadcasts m and e to Alice. Alice has a message that consists of a sequence of numerical words. Each word is a number w that is smaller than m. To encrypt the word w, Alice computes

$$c = w^e \pmod{m}.$$

That is, Alice finds the number $c < m$ that is congruent to w^e modulo m. She broadcasts the encrypted word c to Bob. Bob computes

$$w' = c^d \pmod{m}.$$

Then w' will be the original word w of Alice. For since $ed \equiv 1 \pmod{\phi(m)}$, we have

$$w' \equiv c^d \equiv (w^e)^d = w^{1+k\phi(m)} \equiv w \pmod{m}$$

for some integer k, where the last congruence follows from Corollary 16 of Chapter 9. Since both w and w' are numbers less than m, then $w = w'$.

C.3 Types of Primalitiy Tests

As noted in [FR07, p. 213] a primality test is [...] an algorithm that inputs a positive integer n and outputs whether it is prime or composite. These tests can be subclassified as either **deterministic** primality tests or **probabilistic** primality tests. In a deterministic test an integer n is inputted and the output is, yes the integer is prime, or no the integer is not prime. Hence both the direct method of trial division and the sieve of Eratosthenes are deterministic tests. A nondeterministic primality test takes an inputted integer n and returns either no it is not prime or it may be a prime. A probabilistic primality test is a nondeterministic test that returns either that the inputted integer is not a prime or that is probably a prime to some given degree of likelihood. There are various tests [...] that can give this likelihood to as high a probability as desired, like the **Solovay-Strassen test** and the **Miller-Rabin test**.
[FR07, p. 218] continues in saying the basic idea in both of these is to test, for an inputted integer n, a sequence of bases in the Fermat test. The hope is that a base will be located for which the test fails. In this case the number is not prime. If no such base is found a probability can be assigned, determined by the number of bases tested, that the number is prime.

C.4 Probable Prime and Industrial Grade Prime

As written in [FR07, p. 213] numbers that pass a probabilistic primality test are called **probable primes**. For use in cryptography, knowing whether an integer is prime to a high probability is often just as good as knowing if it is definitely prime. For this reason, probable primes with a high degree of probability are called industrial grade primes, a term originally coined by M. Cohen.

References

[AGP94a] W. R. Alford, A. Granville, and C. Pomerance, *On the difficulty of finding reliable witnesses*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 877, 1994, pp. 1–16.

[AGP94b] ———, *There are infinitely many Carmichael numbers*, Ann. of Math. **140** (1994), 703–722.

[Art67] M. Artjuhov, *Certain criteria for the primality of numbers connected with the little Fermat theorem*, Acta Arith. **12** (1966/67), 355–364, (in Russian).

[Bac85] E. Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, ACM Distinguished Dissertation, The MIT Press, 1985.

[Bee51] N.G.W.H. Beeger, *On even numbers m dividing* $2^m - 2$, Amer. Math. Monthly **58** (1951), 553–555.

[BLS+88] J. Billhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Jr. Wagstaff, *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2 ed., Contemporaray Math., vol. 22, Amer. Math. Soc., 1988.

[BN97] R. Balasubramanian and S. V. Nagaraj, *Density of Carmichael numbers with three prime factors*, Math. Comput. **66** (1997), 1705–1708.

[Bur97] R. Burthe, *Upper bounds for least witnesses and generating sets*, Acta Arith. **80** (1997), 311–326.

[BW80] R. Baillie and S.S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), no. 152, 1391–1417.

[Car12] R. D. Carmichael, *On composite numbers p, which satisfy the Fermat congruence* $a^{P-1} \equiv 1 \pmod{p}$, Amer. Math. Monthly **19** (1912), 22–27.

[Car13] ———, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Math. **15** (1913), no. 2, 30–70.

[Car10] ———, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1909-10), 232–238.

[Che39] H. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), 269–274.

[Chi09] L. N. Childs, *A Concrete Introduction to Higher Algebra*, 3 ed., Undergraduate Texts in Mathematics, Springer Science+Business Media, Inc., 2009.

[Cip04] M. Cipolla, *Sui numeri composti p che verificano la congruenza di Fermat,* $a^{P-1} \equiv 1 \pmod{p}$, Annali di Mathematica **9** (1904), 139–160.

[CP05] R. E. Crandall and C. Pomerance, *Prime Numbers - A Computational Perspective*, 2 ed., Springer Science+Business Media, Inc., New York, 2005.

[Cro62] R. Crocker, *A theorem on pseudo-primes*, Amer. Math. Monthly **69** (1962), 540.

[Dic52] L.E. Dickson, *History of the Theory of Numbers vol. 1 - Divisibility and Primality*, Publication - Carnegie Institution of Washington, Chelsea Publishing Company, 1952.

[Dup53] H. J. A. Duparc, *On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers*, Rapport Zw 1953 - 004, Math. Centrum Amsterdam, 1953.

[Erd49] P. Erdös, *On the converse of Fermat's theorem*, Amer. Math. Monthly **56** (1949), 623–624.

[Erd50] ———, *On almost primes*, Amer. Math. Monthly **57** (1950), 404–407.

[Erd56] ———, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206.

[FK83] J. Fehér and P. Kiss, *Note on super pseudoprime numbers*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **26** (1983), 157–159.

[FR07] B. Fine and G. Rosenberger, *Number Theory - An Introduction via the Distribution of Primes*, Birkhäuser, Boston, 2007.

[Guy04] R. K. Guy, *Unsolved Problems in Number Theory*, 3 ed., Problem Books in Mathematics, Springer-Verlag, 2004.

[Jae90] G. Jaeschke, *The Carmichael numbers up to* 10^{12}, Math. Comp. **55** (1990), 383–389.

[Jae93] ———, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926.

[Jar50] D. Jarden, *Existence of an infinitude of composite n for which* $2^{n-1} \equiv 1 \pmod{n}$, Riveon Lematematika **4** (1950), 65–67.

[Jea98] J.H. Jeans, *The converse of Fermat's theorem*, Messenger of Mathematics **27** (1897/98), 174.

[Kel91] W. Keller, *Whence come the largest presently known primes?*, Math. Ges. Hamburg **12** (1991), 211–229.

[KLS01] M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers - From Number Theory to Geometry*, Springer Verlag, 2001.

[Knö53] W. Knödel, *Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x*, Arch. Math. **4** (1953), 282–284.

[Kor99] A. Korselt, *Probléme chinois*, L'Interm. des Math. **6** (1899), 142–143.

[KPL86] P. Kiss, B.M. Phong, and E. Lieuwens, *On Lucas pseudoprimes which are products of s primes*, Fibonacci Numbers and Their Applications (Dordrecht) (A.N. Philippou, G.E. Bergum, and A.F. Horadam, eds.), Reidel, 1986, pp. 131–139.

[Leh36] D. H. Lehmer, *On the converse of Fermat's theorem I*, Amer. Math. Monthly **43** (1936), 347–354.

[Leh49] ———, *On the converse of Fermat's theorem II*, Amer. Math. Monthly **56** (1949), 300–309.

[Leh76] D.H. Lehmer, *Strong Carmichael numbers*, J. Austral. Math. Soc. A **21** (1976), 508–510.

[Li97] X.-J. Li, *The positivity of a sequence of numbers and the Riemann hypothesis*, J. Number Theory **65** (1997), 325–333.

[Lie71] E. Lieuwens, *Fermat pseudo-primes*, Ph.D. thesis, Delft, 1971.

[Mah13] D. Mahnke, *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung*, Bibliotheca Math. **13** (1913), 29–61.

[Mąk74] A. Mąkowski, *On a problem of Rotkiewicz on pseudoprimes*, Elem. Math. **29** (1974), 13.

[Mal03] E. Malo, *Nombres qui, sans être premiers, vérifient exceptionnellement une congruence de Fermat*, L'Interm. des Math. **10** (1903), 88.

[Mal77] D. E. G. Malm, *On Monte-Carlo primality testing*, Notices Amer. Math. Soc. **24** (1977), A–529.

[Mil76] G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), 300–317.

[Mon80] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theor. Comput. Sci. **12** (1980), 97–108.

[Pin92] R. G. E. Pinch, *The pseudoprimes up to* 10^{12}, unpublished manuscript, 1992.

[Pin93] ———, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391.

[Pin98] ———, *The Carmichael numbers up to* 10^{16}, preprint, 1998.

[Pin00] ———, *The pseudoprimes up to* 10^{13}, Proc. Fourth Int. Symp. on Algorithmic Number Theory (W. Bosma, ed.), Lecture Notes in Computer Sci., no. 1838, Springer Verlag, 2000, pp. 459–474.

[Pom81] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.

[Pom82] ———, *A new lower bound for the pseudoprimes counting function*, Illinois J. Math. **26** (1982), 4–9.

[Pou38] P. Poulet, *Table de nombres copmosés vérifiant le théorème de Fermat pour le module 2 jusq'à 100 000 000*, Sphinx **8** (1938), 42–52.

[PSW80] C. Pomerance, J. L. Selfridge, and S. S. Jr. Wagstaff, *The pseudoprimes to* 25×10^9, Math. Comp. **35** (1980), 1003–1026.

[Rab76] M. O. Rabin, *Probabilistic algorithms*, In Algorithms and Complexity, 1976, pp. 21–39.

[Rab80] ———, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138.

[Rib04] P. Ribenboim, *The little Book of Bigger Primes*, 2 ed., Springer Verlag, 2004.

[Rie94] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2 ed., Progress in Mathematics, vol. 126, Birkhäuser, Boston, 1994.

[Rot59a] A. Rotkiewicz, *Sur le nombres coposés n qui divisent* $a^{n-1}-b^{n-1}$, Rendiconti del Circolo Matematico di Palermo **8** (1959), 115–116.

[Rot59b] ———, *Sur le nombres pairs n pour lesquels les nombres* a^nb-ab^n*, respectivement* $a^{n-1}-b^{n-1}$*, sont divisibles par n*, Rendiconti del Circolo Matematico di Palermo **8** (1959), 341–342.

[Rot63] ———, *Sur les nombres pseudo premiers de la frome* $ax + b$, C. R. Acad. Sci., Paris, Sér. I, Math. **257** (1963), 2601–2604.

[Rot64] ———, *Sur les formules donnant des nombres pseudopremiers*, Colloq. Math. **12** (1964), 69–72.

[Rot65] ———, *Les intervalles contenant les nombres pseudopremiers*, Rend. Circ. Mat. Palermo **14** (1965), 278–280.

[Rot67] ———, *On the pseudoprimes of the form* $ax+b$, Proc. Cambridge Philos. Soc. **63** (1967), 389–392.

[Rot68] ———, *On the prime factors ot the numbers* $2^{p-1} - 1$, Glasgow Mathematical Journal **9** (1968), 83–86.

[Rot72] ———, *Pseudoprime Numbers and their Generalizations*, Stud. Assoc. Fac. Sci. Univ. Novi Sad, 1972.

[Sch58] A. Schinzel, *Sur les nombres composés n qui divisent* $a^n - a$, Rend. Circ. Math. Palermo **7** (1958), 1–5.

[Sha78] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 2 ed., Chelsea Publishing Company, New York, 1978.

[Sie47] W. Sierpiński, *Remarque sur une hypothése de chinois concernant le nombres* $(2^n - 2)/n$, Colloq. Math. **1** (1947), 9.

[Sie88] ———, *Elementary Theory of Numbers*, 2 ed., North-Holland Mathematical Library, vol. 31, Elsevier, 1988.

[Som04] L. Somer, *On super-pseudoprimes*, Mathematica Slovaca **54** (2004), 443–451.

[SS77] R. Solovay and V.A. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85.

[Ste48] R. Steuerwald, *Über die Kongruenz* $a^{n-1} \equiv 1 \pmod{n}$, Sitzungsbericht, Math.-naturw. Kl. Bayer. Akad. Wiss. München, München, 1948.

[Swi75] J.D. Swift, *Table of Carmichael numbers to* 10^9, Math. Comp. **29** (1975), 338–339.

[Szy66] K. Szymiczek, *Note on Fermat numbers*, Elem. Math. **21** (1966), 59.

[Szy67] ———, *On pseudoprime numbers which are products of distinct primes*, Amer. Math. Monthly **74** (1967), 35–37.

[Szy65] ———, *On prime numbers* p, q *and* r *such that* pq, pr *and* qr *are pseudoprimes*, Colloq. Math. **13** (1964-65), 259–263.

[Wil78] H.C. Williams, *Primality testing on a computer*, Ars Combinatoria **5** (1978), 127–185.

[Wil98] ———, *Édouard Lucas and primality testing*, Canad. Math. Soc. series of monographs an advanced texts (New York), vol. 22, John Wiley & Sons, 1998.

[WWWa] http://primes.utm.edu/primes/page.php?id=111120 (on 8. 3. 2013).

[WWWb] http://www.mersenne.org/various/57885161.htm (on 8. 3. 2013).

[Yor79] M. Yorinaga, *Search for absolute pseudoprime numbers*, Sûgaku **31** (1979), 374–376.

Curriculum Vitae

Personal

Name:	Birgit Trappl, Bakk.rer.nat. BSc
Date of Birth:	June 27^{th}, 1987
Nationality:	Austria
e-mail:	BirgitTrappl@gmx.at

Education

09/1993 - 06/1997	Primary School (VS St. Georgen am Steinfelde, Niederösterreich)
09/1997 - 06/2001	Middle School (HS St. Georgen am Steinfelde, Niederösterreich)
09/2001 - 06/2005	High School (BRG/BORG St. Pölten, Niederösterreich)
12/2004	Certificate in Advanced English (CAE)
06/2005	A-Levels (Matura) with distinction
10/2005 - 04/2013	Diploma Studies in Mathematics at the University of Vienna
10/2005 - 07/2012	Diploma Studies in Physics at the University of Vienna
10/2007 - 09/2010	Bachelor Studies in Astronomy at the University of Vienna
09/2007	Award of academic degree Bakk.rer.nat. in Astronomy with distinction
12/2007	First diploma examination in Mathematics
07/2008	First diploma examination in Physics with distinction
06/2012	Second diploma examination in Physics with distinction
07/2012	First part of second diploma examination in Mathematics
07/2012	Award of academic degree BSc in Physics
Since 07/2012	Master Studies in Physics at the University of Vienna

Conferences and Workshops

30/09 - 01/10/2010	CoQuS II kick-off workshop (Vienna)
04/11 - 07/11/2010	14. Deutsche Physikerinnentagung (Munich)